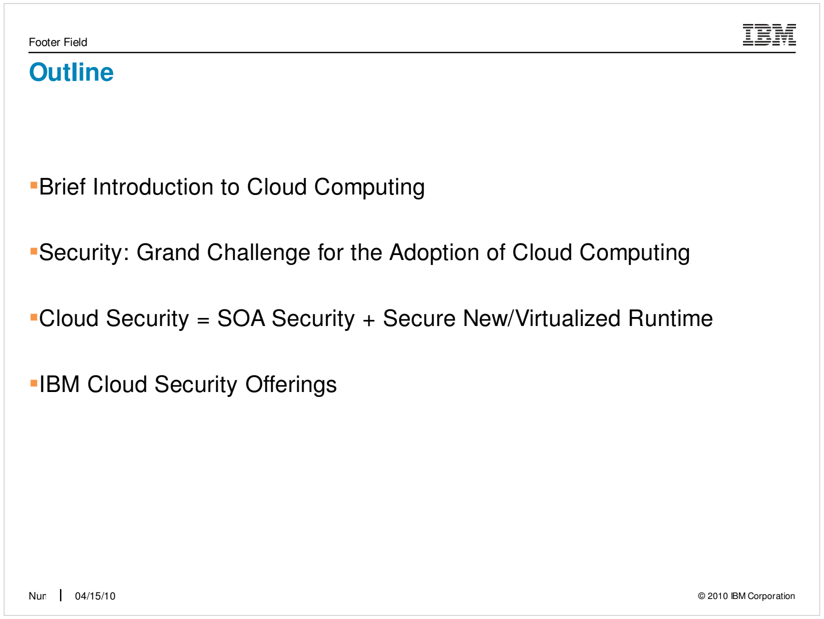
Scott Henley
WW Security Tiger Team
AP IBM Tivoli Security Technical Leader
scott.henley@au1.ibm.com

Security and Cloud Computing

04/15/10

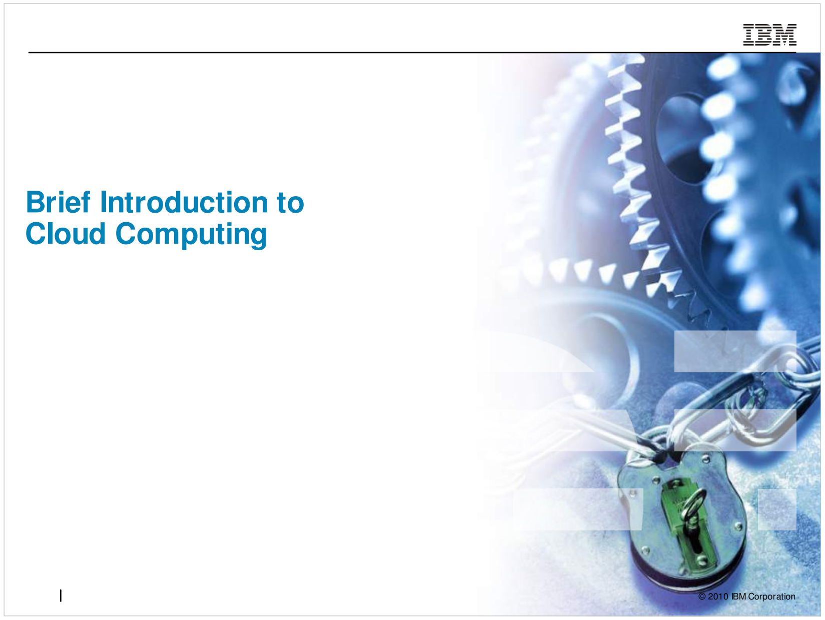
© 2010 IBM Corporation



Outline

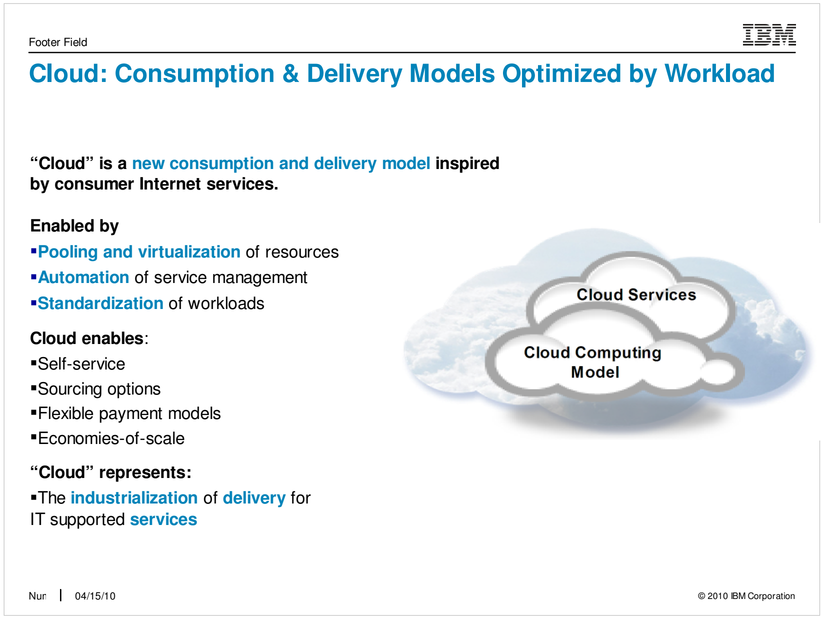
- Brief Introduction to Cloud Computing
- Security: Grand Challenge for the Adoption of Cloud Computing
- Cloud Security = SOA Security + Secure New/Virtualized Runtime
- IBM Cloud Security Offerings

© 2010 IBM Corporation



Brief Introduction to Cloud Computing

© 2010 IBM Corporation



Cloud: Consumption & Delivery Models Optimized by Workload

"Cloud" is a new consumption and delivery model inspired by consumer Internet services.

Enabled by

- **Pooling and virtualization** of resources
- **Automation** of service management
- **Standardization** of workloads

Cloud enables:

- Self-service
- Sourcing options
- Flexible payment models
- Economies-of-scale

"Cloud" represents:

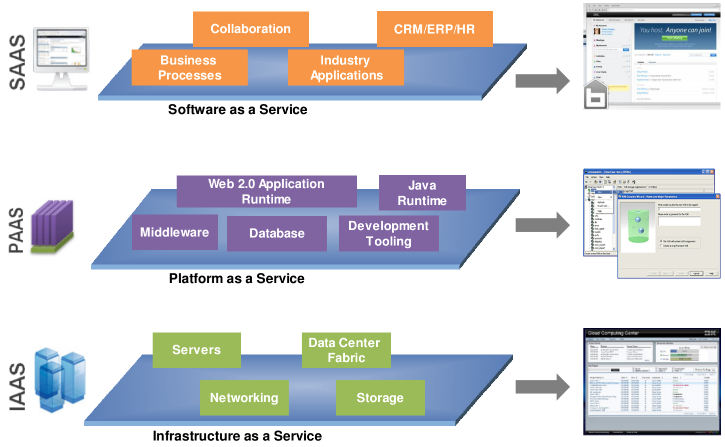
- The **industrialization** of **delivery** for IT supported **services**

Cloud Services

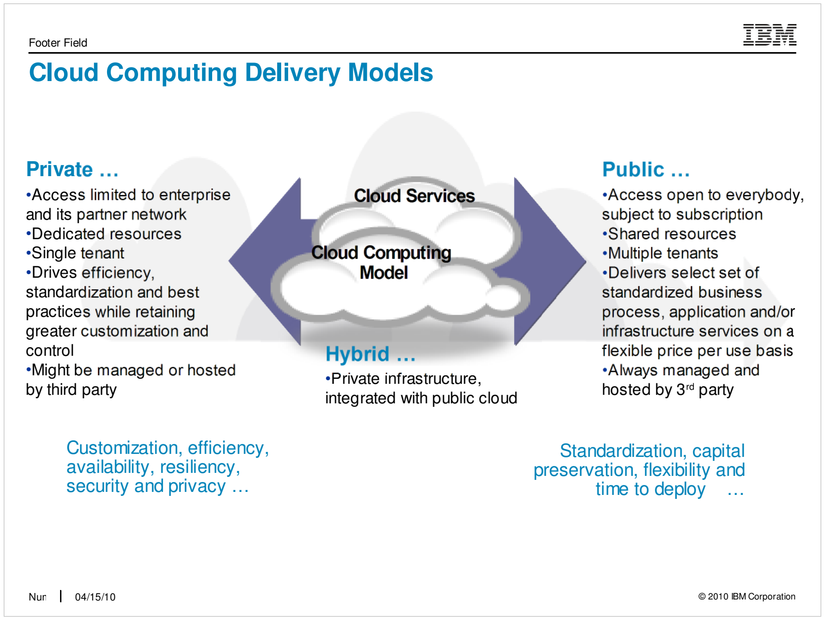
Cloud Computing Model

© 2010 IBM Corporation

The Layers of IT-as-a-Service



© 2010 IBM Corporation



Cloud Computing Delivery Models

Cloud Services

Cloud Computing Model

Private …

- Access limited to enterprise and its partner network
- Dedicated resources
- Single tenant
- Drives efficiency, standardization and best practices while retaining greater customization and control
- Might be managed or hosted by third party

Hybrid …

- Private infrastructure, integrated with public cloud

Public …

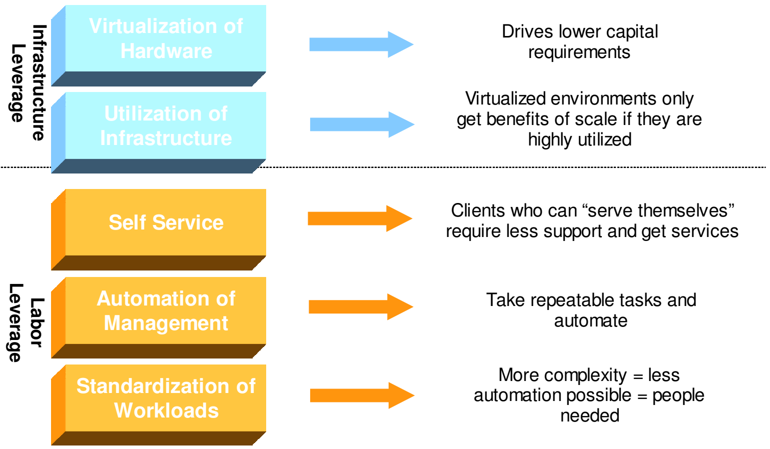
- Access open to everybody, subject to subscription
- Shared resources
- Multiple tenants
- Delivers select set of standardized business process, application and/or infrastructure services on a flexible price per use basis
- Always managed and hosted by 3rd party

Customization, efficiency, availability, resiliency, security and privacy …

Standardization, capital preservation, flexibility and time to deploy …

© 2010 IBM Corporation

These Factors Plus Re-Engineering IT Business and Delivery Processes Drive Cloud Economics



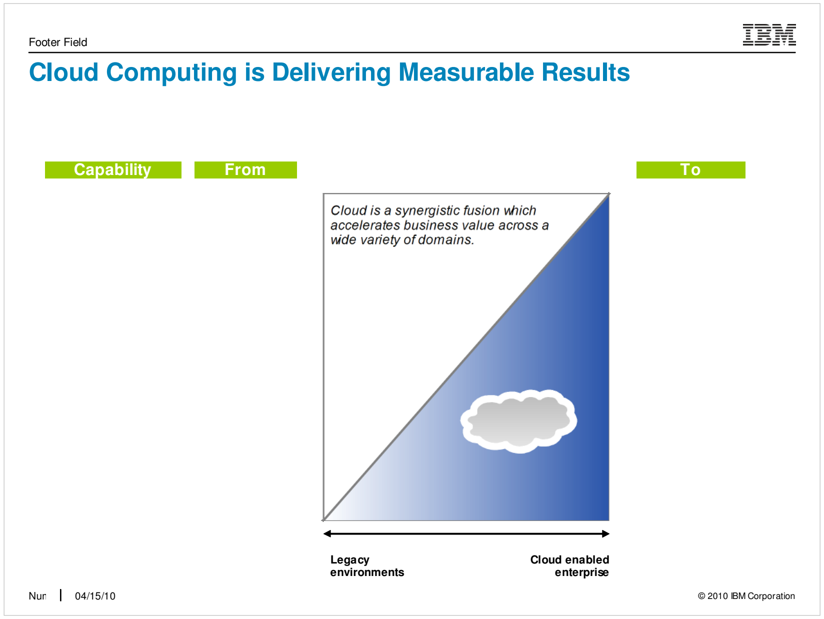
Infrastructure Leverage

- Virtualization of Hardware → Drives lower capital requirements
- Utilization of Infrastructure → Virtualized environments only get benefits of scale if they are highly utilized

Labor Leverage

- Self Service → Clients who can “serve themselves” require less support and get services
- Automation of Management → Take repeatable tasks and automate
- Standardization of Workloads → More complexity = less automation possible = people needed

© 2010 IBM Corporation



Footer Field

Cloud Computing is Delivering Measurable Results

Capability

From

To

Cloud is a synergistic fusion which accelerates business value across a wide variety of domains.

Legacy environments

Cloud enabled enterprise

Nur | 04/15/10

© 2010 IBM Corporation

•The chart depicts the common attributes of cloud computing we discussed earlier and the associated business impact of what a cloud-enabled enterprise can provide..

Virtualization has been around for 30 years. And yet how many have really truly virtualized at all the layers of the stack? You really can't expect cloud to produce what a cloud is expected to produce if in fact it isn't virtualized and standardized and automated, because people expect scalable services, right?

In a cloud environment people, expect self- service, being able to get started very quickly. Self- provisioning or rapid provisioning. All of those things essentially demand that you do have these very important fundamentals in place.

The only way you're going to be able to get efficiency is to virtualize, standardize and automate. And that's going to drive down costs and it's going to improve service. That's really a pretty simple equation and we are seeing clients that are doing this achieve very real measurable business results. These are the type of results we are seeing..

These include

•**Server/storage.** IT resources from servers to storage, network and applications are pooled and virtualized to help provide an implementation-independent, efficient infrastructure, with **Elastic scaling** – environments that can scale up and down by large factors as demand changes.

Automation with :

•**Self-service portal – point and click access to IT resources**

•**Automated provisioning. Re**sources are provisioned on demand, helping to reduce IT resource setup and configuration cycle times

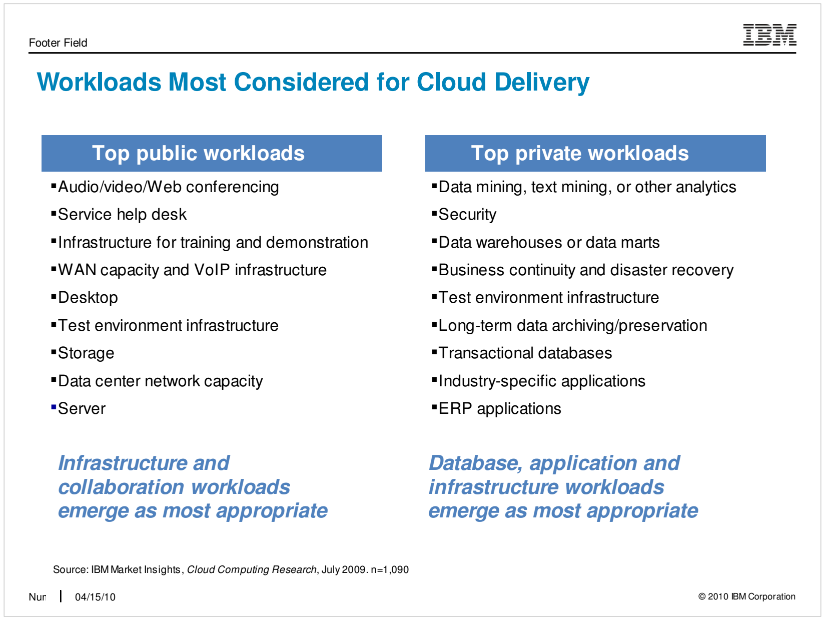
•**Service catalog ordering.** Uniform offerings are readily available from a services catalog on a metered basis.

Standardization with

•**Service catalog ordering.** Uniform offerings are readily available from a services catalog on a metered basis.

•**Flexible pricing.** Utility pricing, variable payments, pay-by-consumption with metering and subscription models help make pricing of IT services more flexible.

Coaching tip - This chart highlights our the real business impact of working with IBM and leveraging cloud computing. They numbers cited can be backed up with testimonials from actual clients. These are "typical results" - this is not marketing hype!



Footer Field

Workloads Most Considered for Cloud Delivery

Top public workloads	Top private workloads
▪Audio/video/Web conferencing	▪Data mining, text mining, or other analytics
▪Service help desk	▪Security
▪Infrastructure for training and demonstration	▪Data warehouses or data marts
▪WAN capacity and VoIP infrastructure	▪Business continuity and disaster recovery
▪Desktop	▪Test environment infrastructure
▪Test environment infrastructure	▪Long-term data archiving/preservation
▪Storage	▪Transactional databases
▪Data center network capacity	▪Industry-specific applications
▪Server	▪ERP applications

Infrastructure and collaboration workloads emerge as most appropriate

Database, application and infrastructure workloads emerge as most appropriate

Source: IBM Market Insights, *Cloud Computing Research*, July 2009. n=1,090

Nur | 04/15/10

© 2010 IBM Corporation

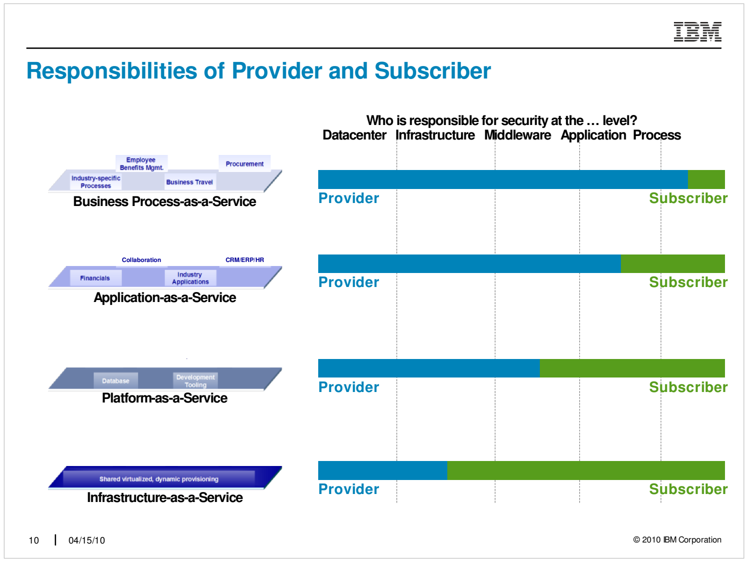
Based on our workload suitability analysis and our experience over the last two years with client engagements and our own internal and public cloud initiatives, IBM has identified the workloads that we believe offer the most favorable entry points for public and for private cloud delivery models.

Moreover, we believe that clients should make workloads a key factor in strategy development for cloud computing.

Put simply, if your organization is interested in piloting a public cloud service, the infrastructure workloads listed here will most likely be the projects that will pose the lowest risk and offer highest potential return.

The same holds true for the workloads listed as top candidates for private cloud implementation.

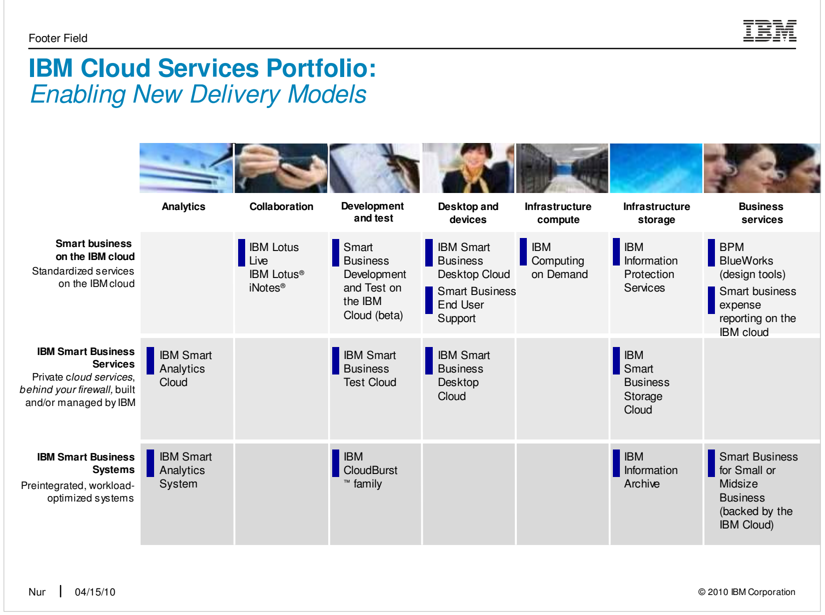
You will notice that "test environment infrastructure" is in the middle of both lists. That is because it is a relatively low-risk workload in terms of the business and the overall IT operation…and at the same time providing test resources using traditional IT delivery is typically slow, costly and a drain on resources, so any gains in speed and reduction in cost translate into a high rate of return. For these reasons, IBM believes that test environment infrastructure should always have high consideration for companies who are looking to choose a pilot cloud project.



Responsibilities of Provider and Subscriber

10 | 04/15/10

© 2010 IBM Corporation



Footer Field

IBM Cloud Services Portfolio:
Enabling New Delivery Models

	Analytics	Collaboration	Development and test	Desktop and devices	Infrastructure compute	Infrastructure storage	Business services
Smart business on the IBM cloud Standardized services on the IBM cloud		IBM Lotus Live IBM Lotus® iNotes®	Smart Business Development and Test on the IBM Cloud (beta)	IBM Smart Business Desktop Cloud Smart Business End User Support	IBM Computing on Demand	IBM Information Protection Services	BPM BlueWorks (design tools) Smart business expense reporting on the IBM cloud
IBM Smart Business Services Private *cloud services, behind your firewall,* built and/or managed by IBM	IBM Smart Analytics Cloud		IBM Smart Business Test Cloud	IBM Smart Business Desktop Cloud		IBM Smart Business Storage Cloud	
IBM Smart Business Systems Preintegrated, workload-optimized systems	IBM Smart Analytics System		IBM CloudBurst ™ family			IBM Information Archive	Smart Business for Small or Midsize Business (backed by the IBM Cloud)

Nur | 04/15/10

© 2010 IBM Corporation

To address the demands of a planet that is growing smarter with each passing day, IBM believes organizations must build a dynamic infrastructure where IT becomes the central nervous system across the business. And one of the best ways to make the data center and IT smarter is a workload-optimized approach with integrated service management and flexible delivery choices.

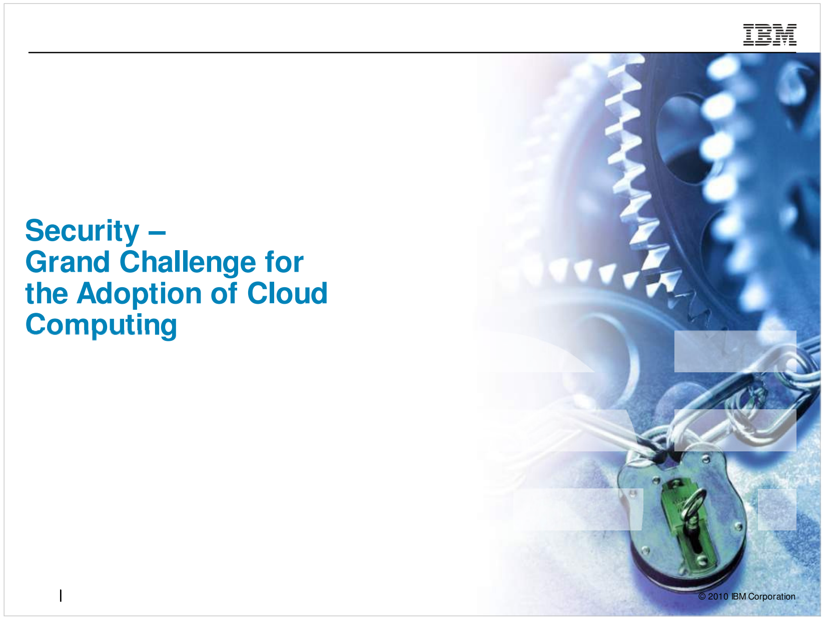
In support of this approach, IBM has introduced and continues to grow a new smart business portfolio that brings together these three differentiators into solutions that your company can leverage today. Our portfolio offers three types of cloud offerings: smart business on the IBM cloud, IBM Smart Business Services and IBM Smart Business Systems.

Lining up our solutions by workload, we're adding capabilities in areas where we already help clients adopt cloud computing with success today. For example:

•IBM Smart Business Desktop Cloud enables a virtualized desktop environment on the IBM cloud. IBM already provides desktop cloud consulting and implementation services. Now clients can have nearly all the benefits of virtual desktops but within a prepriced, prepackaged subscription service.

•IBM Smart Business Storage Cloud allows an enterprise to cost-effectively implement a private storage cloud to handle information that includes, but is not limited to, electronic documents, e-mail and e-mail attachments, presentations, CAD/CAM designs, and source code and Web content from check images to videos, historical documents, medical images, and photographs.

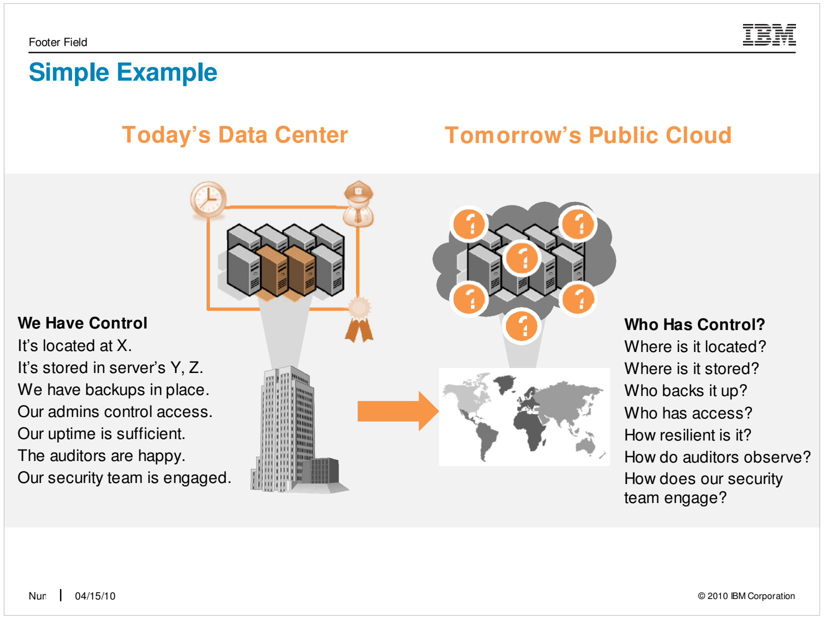
•Announced on June 16, 2009, the IBM CloudBurst™ solution is a self-contained cloud management and resource platform that provides the computing, storage, network and software required for clients to establish a private cloud. The first offering in a family of planned business-ready offerings, the IBM CloudBurst platform includes a self-service portal and a services catalog, helping clients realize rapid time to value. In fact, some clients have had a cloud up and running within hours of installation of the IBM CloudBurst platform. IBM Global Technology Services provides quick-start services to help you assist your clients in gaining the full benefit of the solution.



Security – Grand Challenge for the Adoption of Cloud Computing

l

© 2010 IBM Corporation



Footer Field

Simple Example

Today's Data Center

Tomorrow's Public Cloud

We Have Control

It's located at X.

It's stored in server's Y, Z.

We have backups in place.

Our admins control access.

Our uptime is sufficient.

The auditors are happy.

Our security team is engaged.

Who Has Control?

Where is it located?

Where is it stored?

Who backs it up?

Who has access?

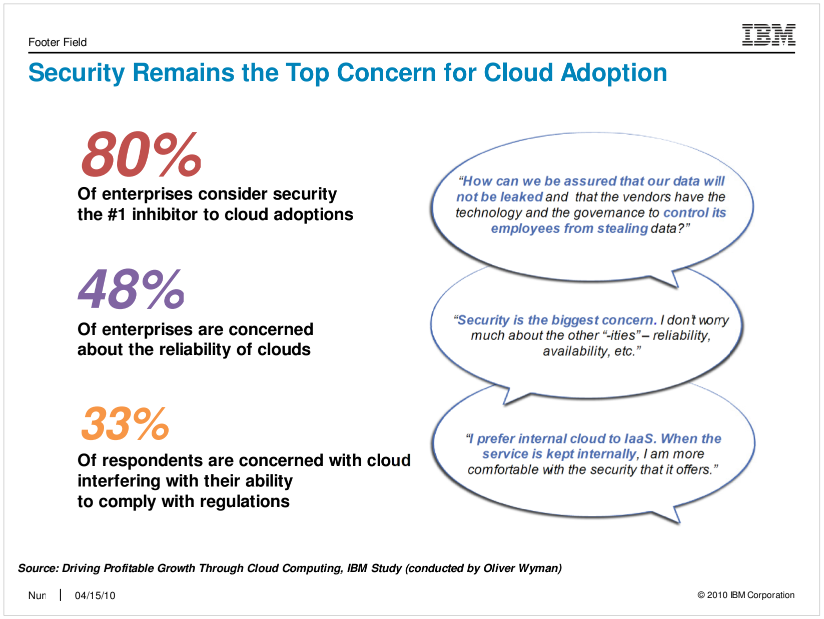
How resilient is it?

How do auditors observe?

How does our security team engage?

Nur | 04/15/10

© 2010 IBM Corporation



Footer Field

IBM

Security Remains the Top Concern for Cloud Adoption

80%

Of enterprises consider security the #1 inhibitor to cloud adoptions

48%

Of enterprises are concerned about the reliability of clouds

33%

Of respondents are concerned with cloud interfering with their ability to comply with regulations

*"**How can we be assured that our data will not be leaked** and that the vendors have the technology and the governance to **control its employees from stealing** data?"*

*"**Security is the biggest concern.** I don't worry much about the other "-ities"– reliability, availability, etc."*

*"**I prefer internal cloud to IaaS. When the service is kept internally**, I am more comfortable with the security that it offers."*

Source: Driving Profitable Growth Through Cloud Computing, IBM Study (conducted by Oliver Wyman)

Nur | 04/15/10

© 2010 IBM Corporation

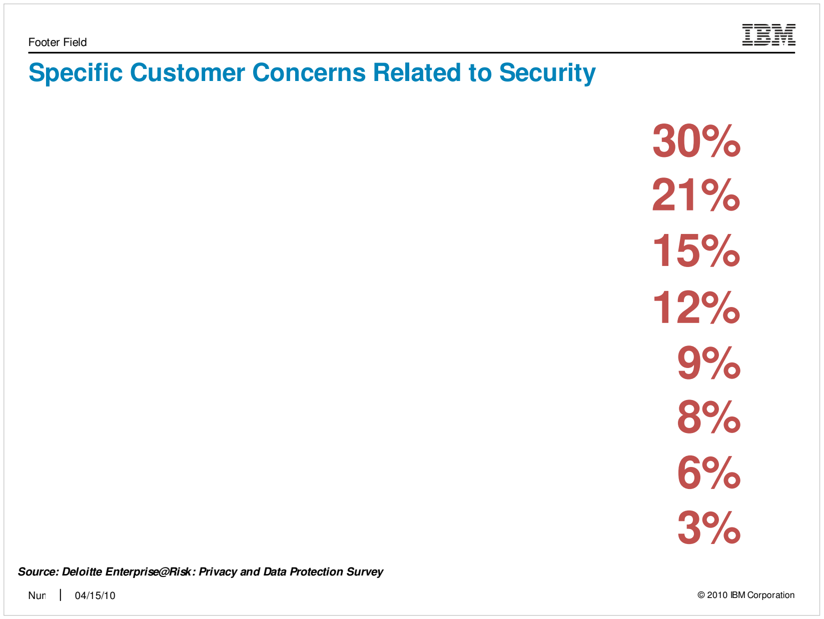
Key point: Based on feedback, security is the #1 concern for customers – as it usually is for any new IT solution.

"External" aspects of the cloud exacerbate this concern, which is why large enterprises resonate with the idea of a private cloud and the degree of control it offers.

▪**Security** is usually the **#1 concern** for any new IT solution, but the additional "external" aspects of the cloud exacerbate this concern

▪Customers were mostly concerned about the data security and the reliability of cloud computing in practice

▪Large enterprises resonated with the concept of Enterprise Cloud which was considered to be more secure than any external solutions



Footer Field

Specific Customer Concerns Related to Security

30%
21%
15%
12%
9%
8%
6%
3%

Source: Deloitte Enterprise@Risk: Privacy and Data Protection Survey

Nur | 04/15/10

© 2010 IBM Corporation

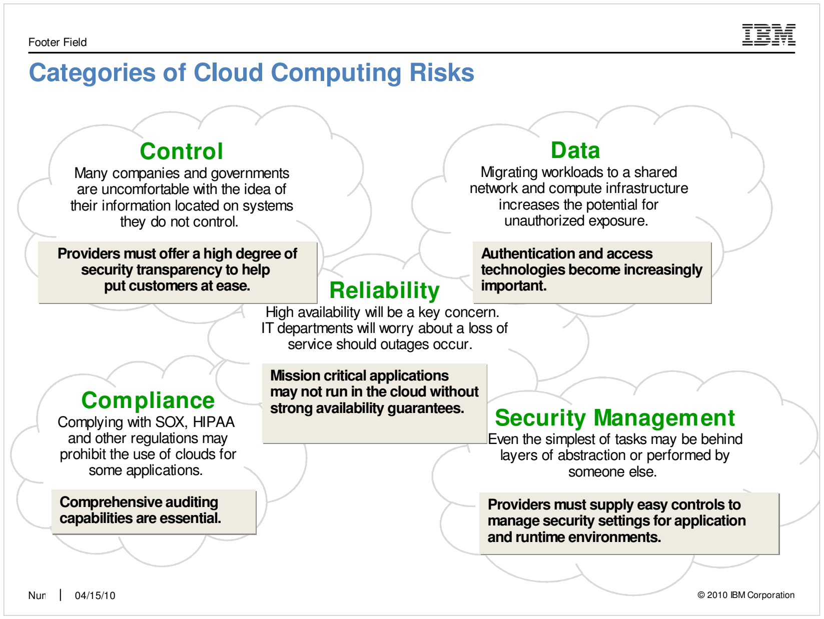
Key Point: As security professionals, our work is cut out for us. Especially since the security concerns related to cloud computing are extremely simple to understand. Here are some examples:

> Losing control over data and operations is unsettling (“External” aspects of public clouds exacerbate this concern).

> Data transferred to a third party can be modified, lost, or stolen.

> A shared, multi-tenant infrastructure increases potential for unauthorized exposure.

> Service disruptions can have tremendous affects the business.



Footer Field

Categories of Cloud Computing Risks

Control

Many companies and governments are uncomfortable with the idea of their information located on systems they do not control.

Providers must offer a high degree of security transparency to help put customers at ease.

Data

Migrating workloads to a shared network and compute infrastructure increases the potential for unauthorized exposure.

Authentication and access technologies become increasingly important.

Reliability

High availability will be a key concern. IT departments will worry about a loss of service should outages occur.

Mission critical applications may not run in the cloud without strong availability guarantees.

Compliance

Complying with SOX, HIPAA and other regulations may prohibit the use of clouds for some applications.

Comprehensive auditing capabilities are essential.

Security Management

Even the simplest of tasks may be behind layers of abstraction or performed by someone else.

Providers must supply easy controls to manage security settings for application and runtime environments.

Nur | 04/15/10

© 2010 IBM Corporation

Key point: Some concerns are more relevant to the cloud than others, these are the most frequently discussed.

Less control: Uncomfortable with the idea of their information on systems they do not own in-house.

Data Security: A shared, multi-tenant infrastructure increases potential for unauthorized exposure. Especially in the case of public-facing clouds.

Reliability: They are worried about service disruptions affecting the business.

Compliance: Regulations may prohibit the use of clouds for certain workloads and data.

Security Management: How will today's enterprise security controls be represented in the cloud?

Top Security Threats and Risks

Gartner: Top Risks (2008)

- Privileged user access
- Regulatory compliance
- Data location
- Data segregation
- Recovery
- Investigative support
- Long-term viability

Soure: Gartner Research, 2008

CSA: Top Threats (2010)

- Abuse and nefarious use of cloud
- Insecure interfaces and APIs
- Malicious insiders
- Shared technology issues
- Data loss or leakage
- Account or service hijacking
- Unknown risk profile

Source: Cloud Security Alliance, 2010

ENISA: Top Risks (2009)

- Loss of governance
- Lock-in
- Isolation failure
- Compliance risks
- Management interface compromise
- Data protection
- Insecure or incomplete data deletion
- Malicious insider

Source: European Network and Information Security Agency, 2009

Synthesis:

- Isolation and multi-tenancy
- Malicious insiders
- Management interface compromise
- Insecure interfaces and APIs
- Data location
- Data protection and security
- Data recovery
- Insecure or incomplete data deletion
- Account or service hijacking
- Abuse of cloud services
- Compliance risks
- Standards-based security

© 2010 IBM Corporation

Recent Analyst Reports Confirm General Concerns – But also Highlight Security as a Potential Market Differentiator

- *"Securing your applications or data when they live in a cloud provider's infrastructure is a complicated issue because you* ***lack visibility and control*** *over how things are being done inside someone else's network."* Forrester, 5/09

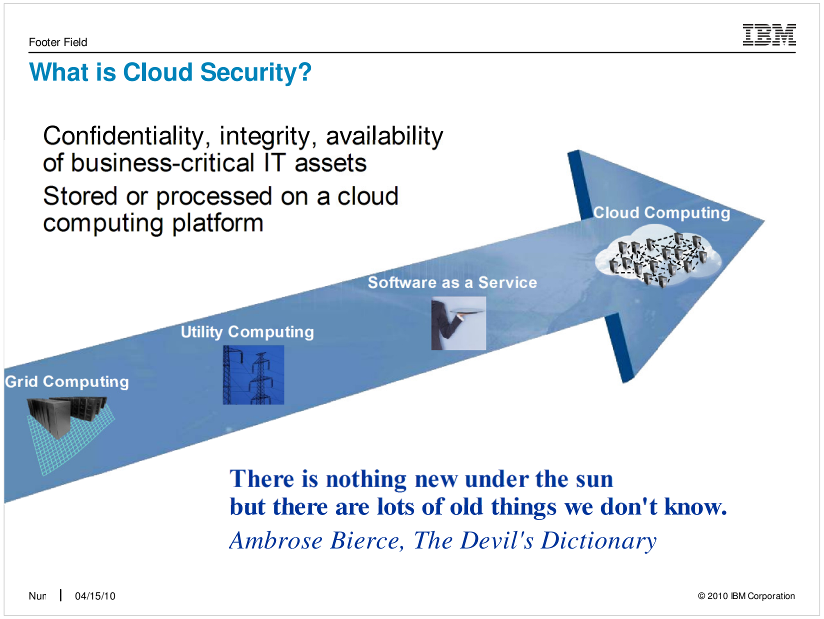
- *"Large enterprises should generally* ***avoid placing sensitive information in public clouds****, but* ***concentrate on building internal cloud and hybrid cloud*** *capabilities in the near term."* Burton, 7/09

- *"Cloud approaches offer a* ***unique opportunity to shift a substantial burden for keeping up with threats to a provider*** *for whom security may well be part of the value proposition."* EMA, 2/09

- Gartner's 7/09 *"Hype Curve for Cloud Computing"* positions Cloud Security Concerns into the ***early phase*** (technology trigger, will raise), and gives it a time horizon of ***5-10 years***

- ***"Highly regulated or sensitive proprietary information should not be stored or processed in an external public cloud-based service*** *without appropriate visibility into the provider's technology and processes and/or the use of encryption and other security mechanisms to ensure the appropriate level of information protection."* Gartner 7/09

© 2010 IBM Corporation



Footer Field

What is Cloud Security?

Confidentiality, integrity, availability of business-critical IT assets

Stored or processed on a cloud computing platform

Grid Computing

Utility Computing

Software as a Service

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

Nur | 04/15/10

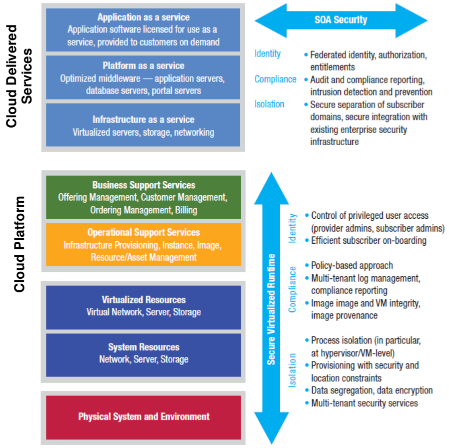
© 2010 IBM Corporation

Cloud Security =

SOA Security +
Secure New/Virtualized Runtime

© 2010 IBM Corporation

Cloud Security = SOA Security + Secure Virtualized Runtime



Cloud Delivered Services

Application as a service
Application software licensed for use as a service, provided to customers on demand

Platform as a service
Optimized middleware — application servers, database servers, portal servers

Infrastructure as a service
Virtualized servers, storage, networking

SOA Security

Identity
- Federated identity, authorization, entitlements

Compliance
- Audit and compliance reporting, intrusion detection and prevention

Isolation
- Secure separation of subscriber domains, secure integration with existing enterprise security infrastructure

Cloud Platform

Business Support Services
Offering Management, Customer Management, Ordering Management, Billing

Operational Support Services
Infrastructure Provisioning, Instance, Image, Resource/Asset Management

Virtualized Resources
Virtual Network, Server, Storage

System Resources
Network, Server, Storage

Physical System and Environment

Secure Virtualized Runtime

Identity
- Control of privileged user access (provider admins, subscriber admins)
- Efficient subscriber on-boarding

Compliance
- Policy-based approach
- Multi-tenant log management, compliance reporting
- Image image and VM integrity, image provenance

Isolation
- Process isolation (in particular, at hypervisor/VM-level)
- Provisioning with security and location constraints
- Data segregation, data encryption
- Multi-tenant security services

Three examples:

IBM Tivoli Federated Identity Manager

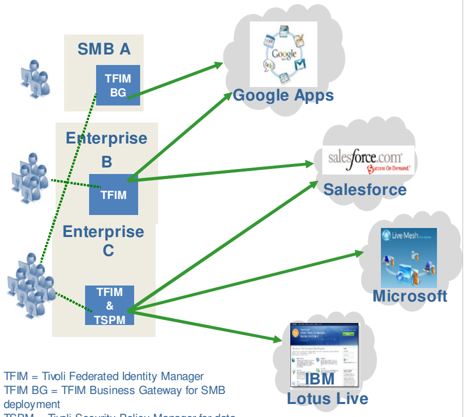
Tivoli Security Information and Event Manager

IBM Security Virtual Server Protection

© 2010 IBM Corporation

Example 1: IBM Tivoli Federated Identity Manager

- Centralized user access management to on- and off-premise apps and services
- Wide variety of Federated SSO protocols
- SAML 1.0 / 1.1 / 2.0
- WS-Federation
- Liberty ID-FF 1.1/ 1.2
- Information Card Profile 1.0
- OpenID
- Integration with IBM LotusLive, Google Apps, salesforce.com, etc.
- Tools for user enrollment, WS-Trust based security token services, web access management
- Simplify integration across Java, .NET and mainframe environments
- Ability to support customizable points of contact to manage identities across multiple cloud patterns

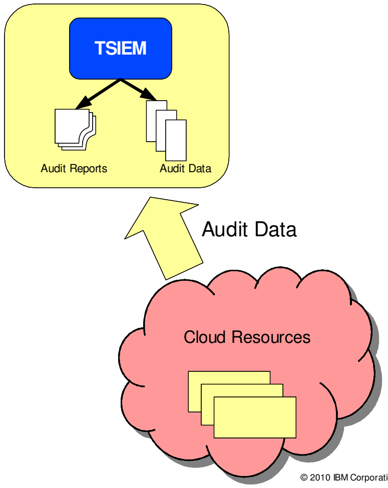


TFIM = Tivoli Federated Identity Manager
TFIM BG = TFIM Business Gateway for SMB deployment
TSPM = Tivoli Security Policy Manager for data entitlement management

© 2010 IBM Corporation

Example 2: IBM Tivoli Security Information and Event Manager

- Gather log files from cloud resources
  - Operating Systems (Linux, AIX, Windows)
  - Databases (Oracle, DB2, ..)
  - Directories (ITDS, AD…)
  - Application Servers (WAS)
  - Network Devices (routers, firewalls,…)
  - Security products (TAMeb, TFIM …)
- Monitor user behavior
  - W7 log normalization translates your logs into business terms
  - Enterprise compliance dashboard
- Compliance management modules and regulation-specific reports
  - SOX
  - Cobit
  - PCI-DSS
  - ISO 27001

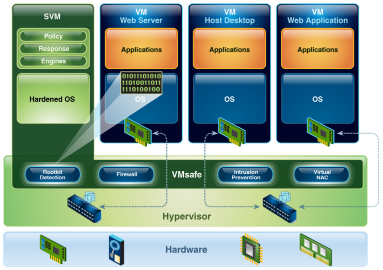


© 2010 IBM Corporation

Example 3: IBM Security Virtual Server Protection for VMware

Integrated threat protection for VMware vSphere 4

Offers broadest, most integrated, defense-in-depth virtualization security with <u>*one product*</u>



- Firewall
- VMsafe Integration
- Rootkit Detection
- Intrusion Detection & Prevention
- Inter-VM Traffic Analysis
- VM Sprawl Management
- Network Policy Enforcement
- Automated Protection for Mobile VMs (VMotion)

- Auto Discovery
- Virtual Infrastructure Auditing (Privileged User Access)
- Virtual Network Segment Protection
- Virtual Network-Level Protection
- Virtual Network Access Control
- Central Management
- Web Application Protection
- Virtual Patch

© 2010 IBM Corporation

Virtualization has many benefits but introduces new complexities

- Virtualization blurs the physical boundaries between systems that are used to separate workloads and those responsible for securing them.
- Virtualization enables mobility of systems and flexible deployment and re-deployment of systems. Manually tracking software stacks and configurations of VMs and images becomes increasingly difficult.

Before Virtualization

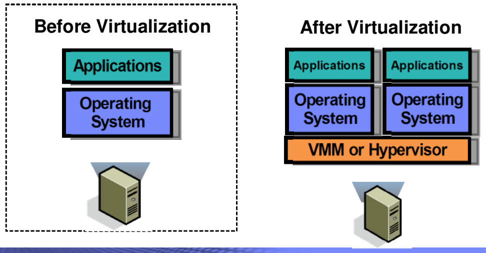
After Virtualization

© 2009 IBM Corporation

Virtualization has many benefits but introduces new complexities

- Virtualization blurs the physical boundaries between systems that are used to separate workloads and those responsible for securing them.

- Virtualization enables mobility of systems and flexible deployment and re-deployment of systems. Manually tracking software stacks and configurations of VMs and images becomes increasingly difficult.



Before Virtualization

Applications

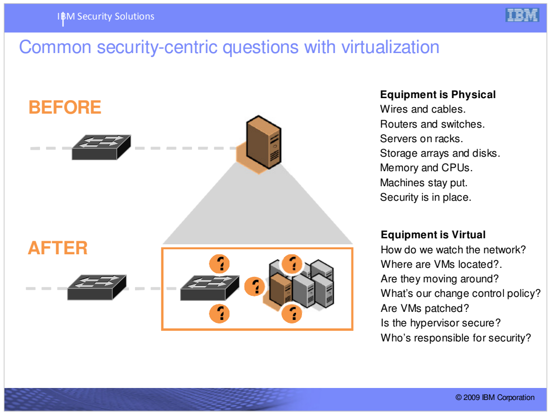
Operating System

After Virtualization

Applications | Applications

Operating System | Operating System

VMM or Hypervisor



IBM Security Solutions

Common security-centric questions with virtualization

BEFORE

AFTER

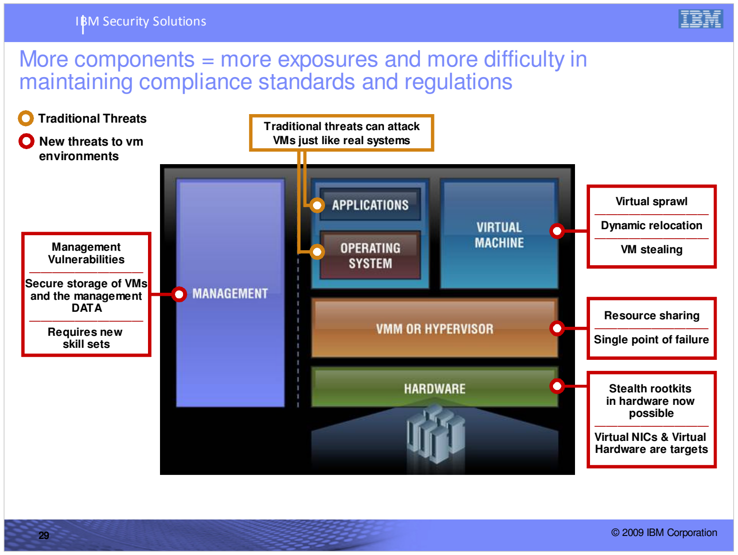
Equipment is Physical
Wires and cables.
Routers and switches.
Servers on racks.
Storage arrays and disks.
Memory and CPUs.
Machines stay put.
Security is in place.

Equipment is Virtual
How do we watch the network?
Where are VMs located?.
Are they moving around?
What's our change control policy?
Are VMs patched?
Is the hypervisor secure?
Who's responsible for security?

© 2009 IBM Corporation

Common security-centric concerns with virtualization

	Physical Network	Virtual Security
Network IPS	Block threats & attacks at perimeter and between network segments	Block threats & attacks on virtual network segments
Server Protection	Secure each physical server with multi-layered protection & reporting on a single agent	Securing each VM as if it were a physical server can mean significant time and cost to system admin
System Patching	Patch critical vulnerabilities on each server and network	Dynamic environments lead to un-patched VMs; Difficult to track VM sprawl and keep VMs patched
Security Policies	Set policies specific to critical applications in each network segment & server	Virtualization often drives variety of OS and apps on a single server, so security policies must be more encompassing – web, data, OS coverage, databases, etc.
Integrate Security w/ Virt. Infrastructure	NA	*New frontier of risk requires dedicated features to protect the hypervisor & assist in VM management*



More components = more exposures and more difficulty in maintaining compliance standards and regulations

○ Traditional Threats

○ New threats to vm environments

Traditional threats can attack VMs just like real systems

Management Vulnerabilities

Secure storage of VMs and the management DATA

Requires new skill sets

Virtual sprawl

Dynamic relocation

VM stealing

Resource sharing

Single point of failure

Stealth rootkits in hardware now possible

Virtual NICs & Virtual Hardware are targets

© 2009 IBM Corporation

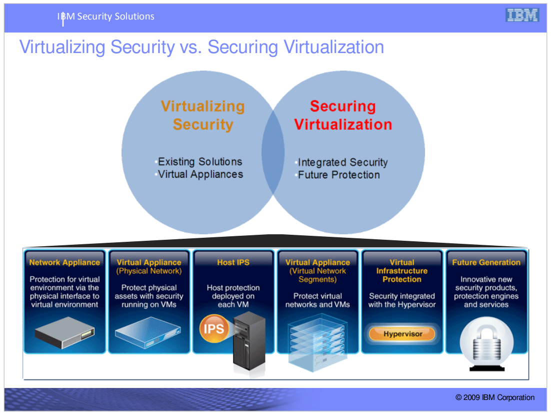
Current best practices for securing virtualization through compliance-oriented internal controls

1. Harden platforms to reduce the risk unauthorized access
2. 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
3. Maintain separate administrative access control although server, network and security infrastructure is now consolidated
4. Provide Virtual machine and virtual network security segmentation
5. Maintain virtual audit logging

Source: RSA Security Brief: Security Compliance in a Virtual World

http://www.rsa.com/solutions/technology/secure/wp/10393_VIRT_BRF_0809.pdf

© 2009 IBM Corporation



Virtualizing Security vs. Securing Virtualization

Virtualizing Security
Existing Solutions
Virtual Appliances
Securing Virtualization
Integrated Security
Future Protection
Network Appliance
Protection for virtual environment via the physical interface to virtual environment
Virtual Appliance (Physical Network)
Protect physical assets with security running on VMs
Host IPS
Host protection deployed on each VM
IPS
Virtual Appliance (Virtual Network Segments)
Protect virtual networks and VMs
Virtual Infrastructure Protection
Security integrated with the Hypervisor
Hypervisor
Future Generation
Innovative new security products, protection engines and services

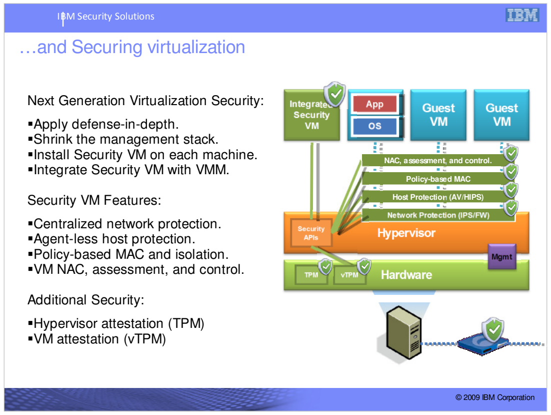
© 2009 IBM Corporation

Virtualizing Security…
IBM Proventia Virtualized Network Security Platform

- Market-leading network protection now available on VMWare virtual platform
  - World class, vulnerability-based protection powered by X-force research
  - "Virtual appliance"
- Protection for virtual environments
  - Intrusion prevention and network protection for traffic between vSwitches
  - Protect the virtual machines on a server
- Integrate and manage virtual security with traditional network security
  - Single management console

Virtual Security Appliances

© 2009 IBM Corporation



…and Securing virtualization

Next Generation Virtualization Security:

- Apply defense-in-depth.
- Shrink the management stack.
- Install Security VM on each machine.
- Integrate Security VM with VMM.

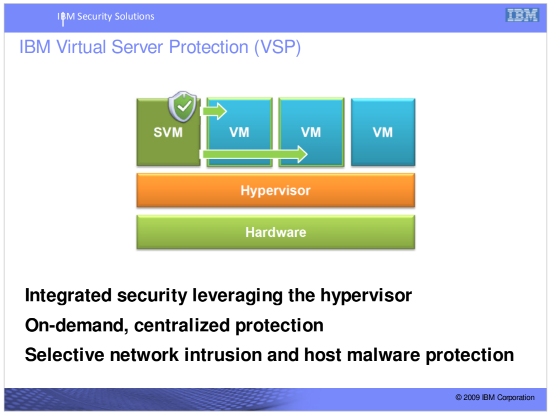
Security VM Features:

- Centralized network protection.
- Agent-less host protection.
- Policy-based MAC and isolation.
- VM NAC, assessment, and control.

Additional Security:

- Hypervisor attestation (TPM)
- VM attestation (vTPM)

© 2009 IBM Corporation



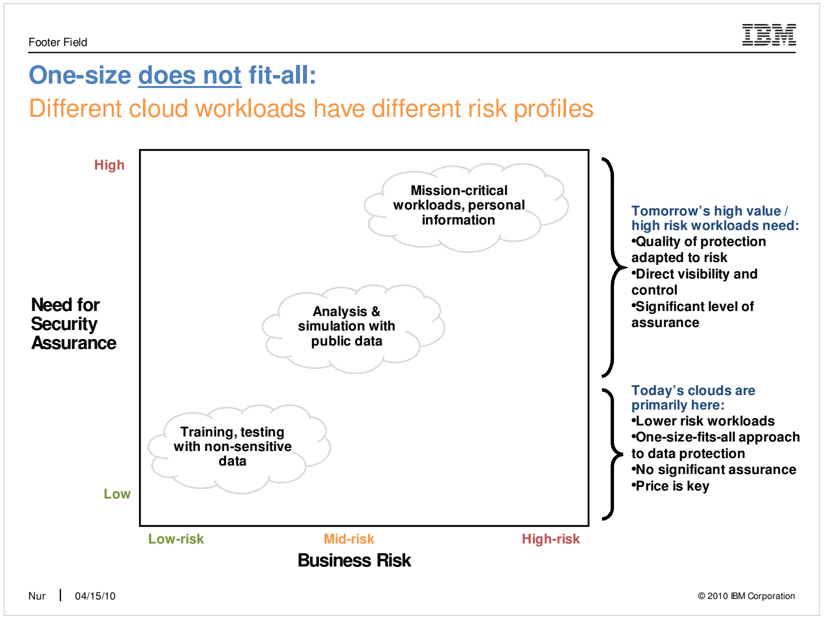
IBM Virtual Server Protection (VSP)

Integrated security leveraging the hypervisor

On-demand, centralized protection

Selective network intrusion and host malware protection

© 2009 IBM Corporation



One-size does not fit-all:

Different cloud workloads have different risk profiles

High

Mission-critical workloads, personal information

Analysis & simulation with public data

Need for Security Assurance

Training, testing with non-sensitive data

Low

Low-risk

Mid-risk

High-risk

Business Risk

Tomorrow's high value / high risk workloads need:

•Quality of protection adapted to risk
•Direct visibility and control
•Significant level of assurance

Today's clouds are primarily here:

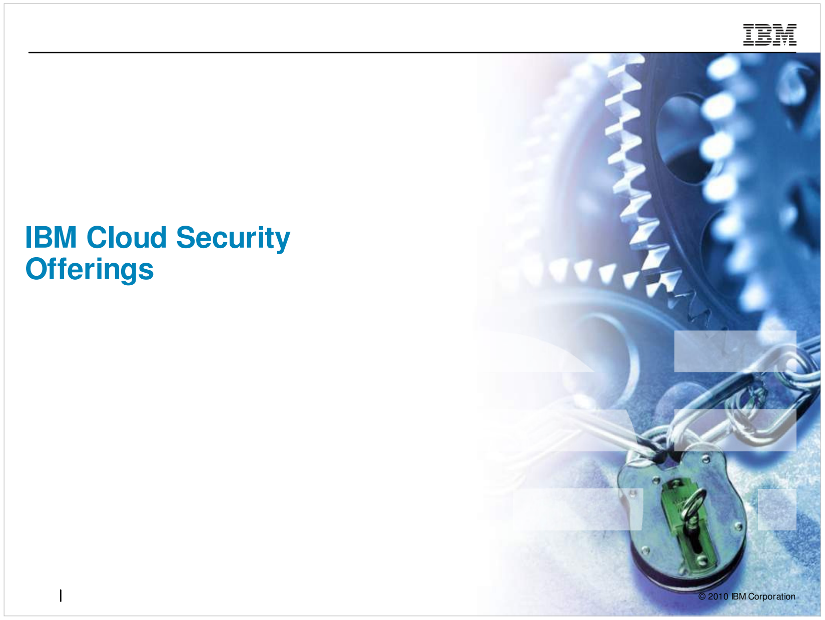
•Lower risk workloads
•One-size-fits-all approach to data protection
•No significant assurance
•Price is key

© 2010 IBM Corporation

Key message: When we talk to our customers about their cloud computing plans, it is apparent that mass adoption of external, massively shared and completely open cloud computing platforms for critical IT services is considered to be still a few years away.

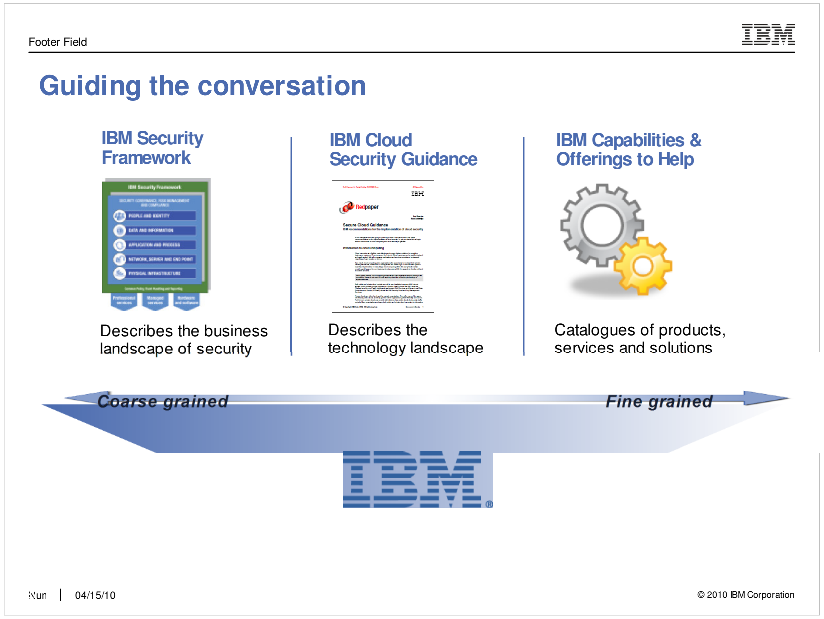
In the near term, most organizations are looking at ways to leverage the services of external cloud providers. These clouds would be used primarily for workloads with a low-risk profile, where a one-size-fits-all approach to security with few assurances is acceptable, and where price is the main differentiator. For workloads with a medium-to-high-risk profile involving highly regulated or proprietary information, organizations are choosing private and hybrid clouds that provide a significant level of control and assurance. These workloads will be shifting into external clouds as they start offering tighter and more flexible security.

Helping to build tomorrow's clouds – that cater to high value / high risk workloads – is an IBM differentiator.



IBM Cloud Security Offerings

© 2010 IBM Corporation



Footer Field

Guiding the conversation

IBM Security Framework

Describes the business landscape of security

IBM Cloud Security Guidance

Describes the technology landscape

IBM Capabilities & Offerings to Help

Catalogues of products, services and solutions

Coarse grained → *Fine grained*

Nur | 04/15/10

© 2010 IBM Corporation

[Self-explanatory]

that security is applied within the organization's process context… meaning the right level of control is enabled at the right layer, at the right time for the organization.

•The multi-dimensional IBM Security Framework represents our belief that today's organizations are complex systems where people interact with applications – residing in a technology infrastructure within a physical facility – often for the purpose of managing data.

•This Framework is designed to:

ide systems and software assurance with the use of secure practices and act

rt FIPS, Common Criteria and similar security validation and certification stan

le innovation and intelligence by securing the infrastructure and helping stay

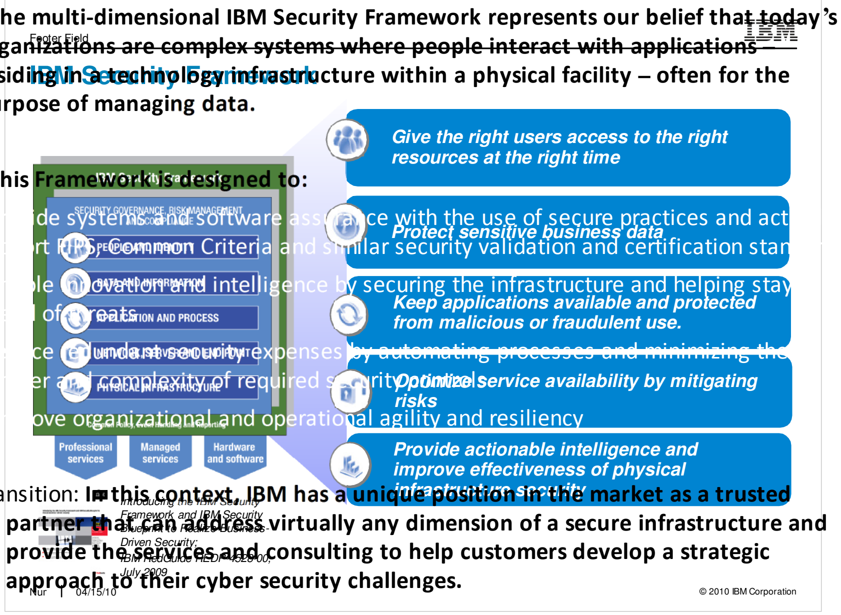
l of threats

ce redundant security expenses by automating processes and minimizing the

er and complexity of required security controls

ove organizational and operational agility and resiliency

Transition: **In this context, IBM has a unique position in the market as a trusted partner that can address virtually any dimension of a secure infrastructure and provide the services and consulting to help customers develop a strategic approach to their cyber security challenges.**



Footer Field

IBM Security Framework

Give the right users access to the right resources at the right time

Protect sensitive business data

Keep applications available and protected from malicious or fraudulent use.

Optimize service availability by mitigating risks

Provide actionable intelligence and improve effectiveness of physical infrastructure security

Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security; IBM RedGuide REDP-4528-00, July 2009

Nur | 04/15/10

© 2010 IBM Corporation

****

<u>Examples of IBM Security offerings and solutions</u> **by Domain, if needed**

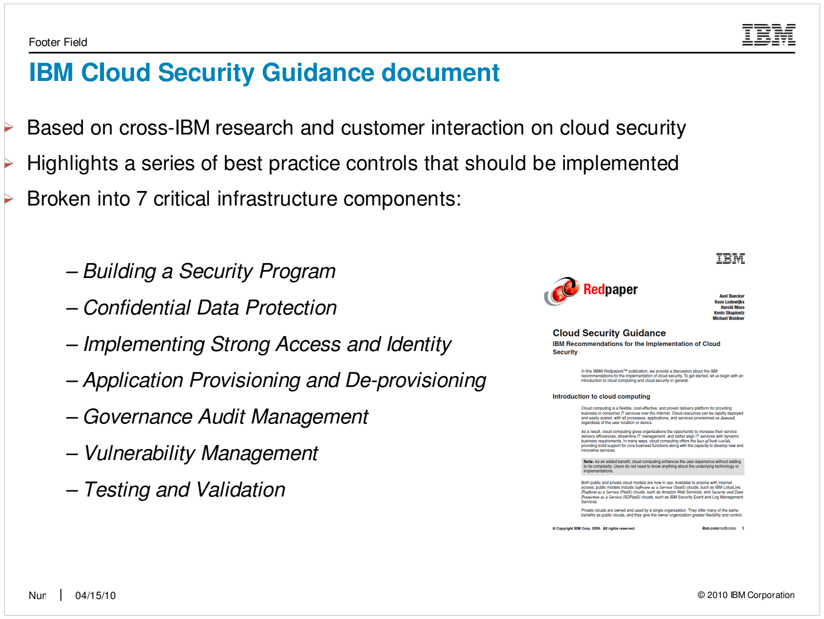
1.People and Identity – Trusted Identity, Identity Provisioning, Identity Proofing, Access Control capabilities inherent in our server and storage platforms

2.Data and Information - Database/Content Management, Content Monitoring, Data Governance, Data Encryption Solutions, Storage Management

3.Application and Process - Secure Development Tools, Security Method Enforcement, Web Application Scanning, Application Firewall, SOA & XML Security

4.Network, Server, and Endpoint - Change & Configuration Mgmt, Intrusion Detection, Vulnerability Mgmt., Event Correlation, Security Compliance Scan, Log management, compliance reporting

5.Physical infrastructure - Digital Video Surveillance, Smart Surveillance Solutions, RFID solutions, Enterprise Asset Mgmt, Physical Security



Footer Field

IBM Cloud Security Guidance document

- Based on cross-IBM research and customer interaction on cloud security
- Highlights a series of best practice controls that should be implemented
- Broken into 7 critical infrastructure components:

  – *Building a Security Program*

  – *Confidential Data Protection*

  – *Implementing Strong Access and Identity*

  – *Application Provisioning and De-provisioning*

  – *Governance Audit Management*

  – *Vulnerability Management*

  – *Testing and Validation*

Redpaper

Axel Buecker
Koos Lodewijkx
Harold Moss
Kevin Skapinetz
Michael Waidner

Cloud Security Guidance

IBM Recommendations for the Implementation of Cloud Security

In this IBM® Redpapers™ publication, we provide a discussion about the IBM recommendations for the implementation of cloud security. To get started, let us begin with an introduction to cloud computing and cloud security in general.

Introduction to cloud computing

Cloud computing is a flexible, cost-effective, and proven delivery platform for providing business or consumer IT services over the Internet. Cloud resources can be rapidly deployed and easily scaled, with all processes, applications, and services provisioned *on demand*, regardless of the user location or device.

As a result, cloud computing gives organizations the opportunity to increase their service delivery efficiencies, streamline IT management, and better align IT services with dynamic business requirements. In many ways, cloud computing offers the *best of both worlds*, providing solid support for core business functions along with the capacity to develop new and innovative services.

Note: As an added benefit, cloud computing enhances the user experience without adding to its complexity. Users do not need to know anything about the underlying technology or implementations.

Both public and private cloud models are now in use. Available to anyone with Internet access, public models include *Software as a Service* (SaaS) clouds, such as IBM LotusLive, *Platform as a Service* (PaaS) clouds, such as Amazon Web Services, and *Security and Data Protection as a Service* (SDPaaS) clouds, such as IBM Security Event and Log Management Services.

Private clouds are owned and used by a single organization. They offer many of the same benefits as public clouds, and they give the owner organization greater flexibility and control.

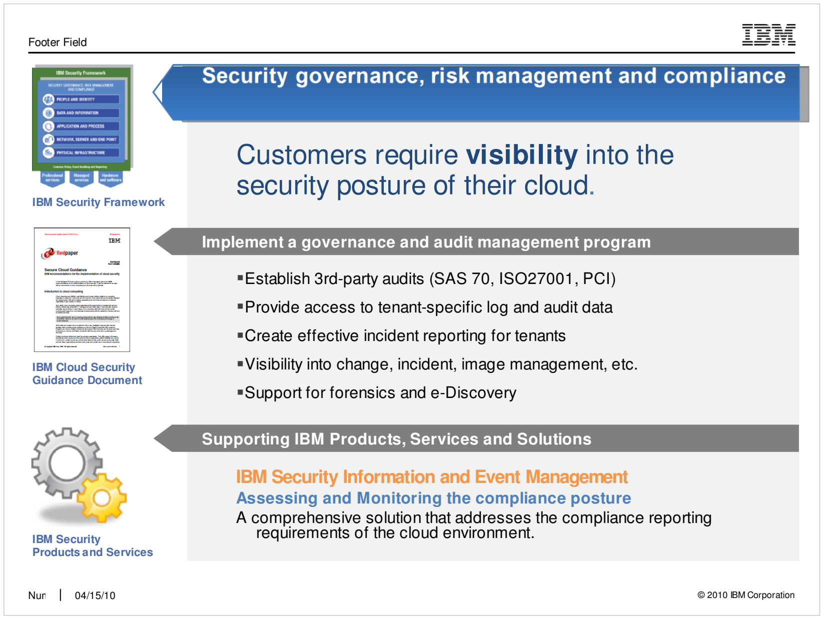
© Copyright IBM Corp. 2009. All rights reserved. ibm.com/redbooks 1

Nur | 04/15/10 © 2010 IBM Corporation

[Self-explanatory]

The following security measures represent general best practice implementations for cloud security.

At the same time, they are not intended to be interpreted as a guarantee of success.



Footer Field

IBM

Security governance, risk management and compliance

IBM Security Framework

Customers require **visibility** into the security posture of their cloud.

IBM Cloud Security Guidance Document

Implement a governance and audit management program

- Establish 3rd-party audits (SAS 70, ISO27001, PCI)
- Provide access to tenant-specific log and audit data
- Create effective incident reporting for tenants
- Visibility into change, incident, image management, etc.
- Support for forensics and e-Discovery

Supporting IBM Products, Services and Solutions

IBM Security Information and Event Management

Assessing and Monitoring the compliance posture

A comprehensive solution that addresses the compliance reporting requirements of the cloud environment.

IBM Security Products and Services

Nur | 04/15/10

© 2010 IBM Corporation

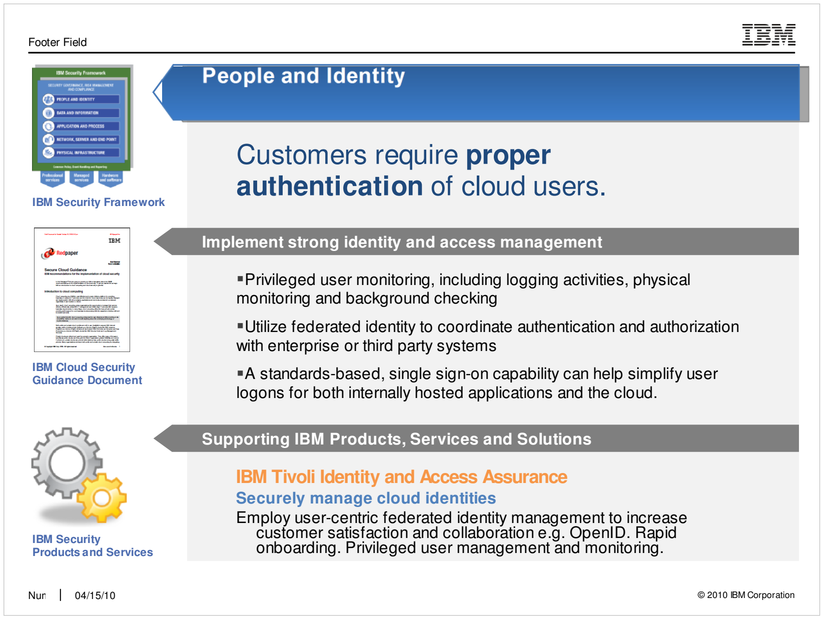
Key Point: From a governance, risk and compliance perspective… organizations require visibility into the security posture of their cloud.

This includes broad-based visibility into change, image, and incident management, as well as incident reporting for tenants and tenant-specific log and audit data.

Visibility can be especially critical for compliance. The Sarbanes-Oxley Act, the Health Insurance Portability and Accountability Act (HIPAA), European privacy laws, and many other regulations require comprehensive auditing capabilities. Since public clouds are by definition a *black box to the subscriber, potential cloud subscribers may not be able to demonstrate* compliance. (A private or hybrid cloud, on the other hand, can be configured to meet those requirements.)

In addition, providers sometimes are required to support third-party audits, and their clients can be directed to support e-Discovery and forensic investigations when a breach is suspected. This adds even more importance to maintaining proper visibility into the cloud.

In general, organizations often cite the need for flexible Service Level Agreements (SLAs) that can be adapted to their specific situation, building on their experiences with strategic outsourcing and traditional, managed services.



Footer Field

People and Identity

Customers require **proper authentication** of cloud users.

IBM Security Framework

Implement strong identity and access management

- Privileged user monitoring, including logging activities, physical monitoring and background checking
- Utilize federated identity to coordinate authentication and authorization with enterprise or third party systems
- A standards-based, single sign-on capability can help simplify user logons for both internally hosted applications and the cloud.

IBM Cloud Security Guidance Document

Supporting IBM Products, Services and Solutions

IBM Tivoli Identity and Access Assurance

Securely manage cloud identities

Employ user-centric federated identity management to increase customer satisfaction and collaboration e.g. OpenID. Rapid onboarding. Privileged user management and monitoring.

IBM Security Products and Services

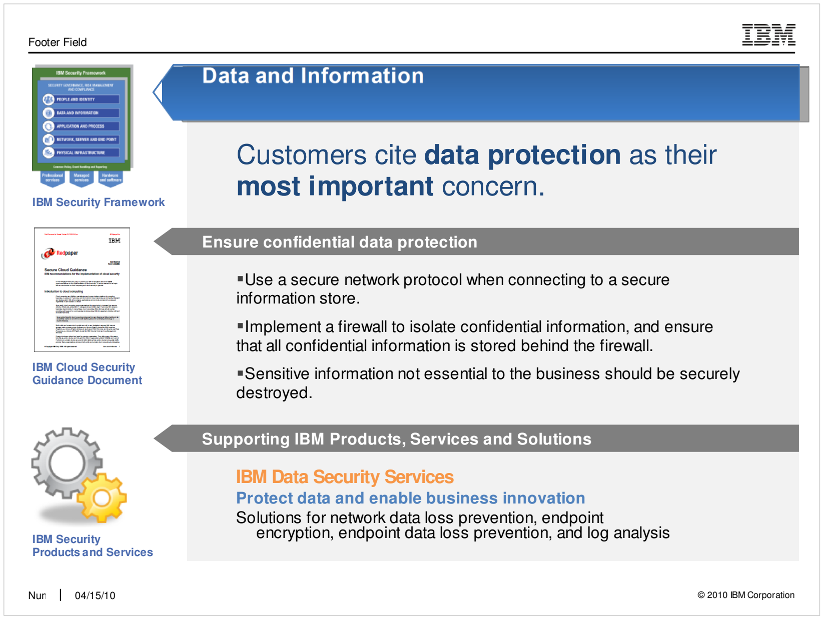
Nur | 04/15/10

© 2010 IBM Corporation

Key Point: Organizations need to make sure that authorized users across their enterprise and supply chain have access to the data and tools that they need, when they need it, while blocking unauthorized access.

Cloud environments usually support a large and diverse community of users, so these controls are even more critical. In addition, clouds introduce a new tier of privileged users: administrators working for the cloud provider. Privileged-user monitoring, including logging activities, becomes an important requirement. This monitoring should include physical monitoring and background checking.

Identity federation and rapid onboarding capabilities must be available to coordinate authentication and authorization with the enterprise back-end or third-party systems. A standards-based, single sign-on capability is required to simplify user logons for both internally hosted applications and the cloud, allowing users to easily and quickly leverage cloud services.



Footer Field

Data and Information

IBM Security Framework

Customers cite **data protection** as their **most important** concern.

Ensure confidential data protection

- Use a secure network protocol when connecting to a secure information store.
- Implement a firewall to isolate confidential information, and ensure that all confidential information is stored behind the firewall.
- Sensitive information not essential to the business should be securely destroyed.

IBM Cloud Security Guidance Document

Supporting IBM Products, Services and Solutions

IBM Data Security Services

Protect data and enable business innovation

Solutions for network data loss prevention, endpoint encryption, endpoint data loss prevention, and log analysis

IBM Security Products and Services

Nur | 04/15/10

© 2010 IBM Corporation

Key Point: Most organizations cite data protection as their most important security issue.

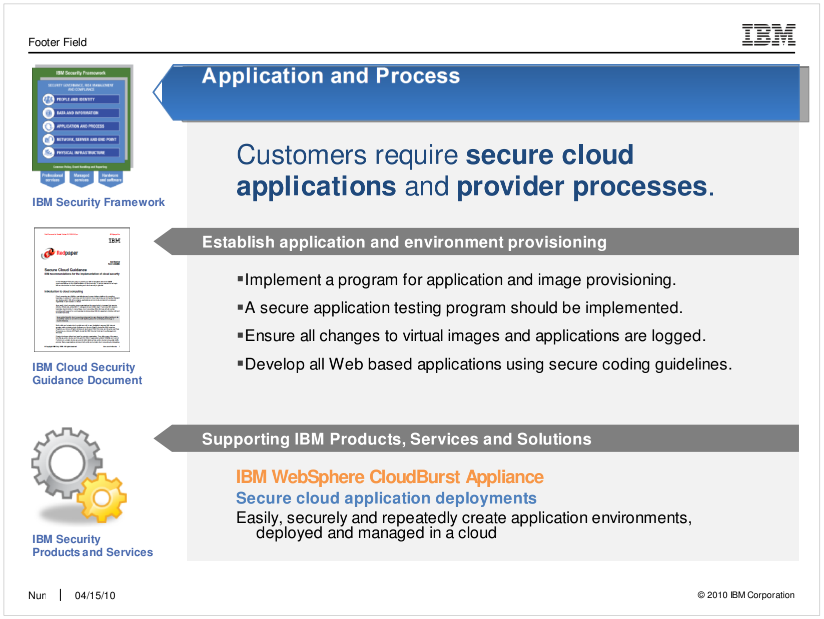
Typical concerns include the way in which data is stored and accessed, compliance and audit requirements, and business issues involving the cost of data breaches, notification requirements, and damage to brand value. All sensitive or regulated data needs to be properly segregated on the cloud storage infrastructure, including archived data.

Encrypting and managing encryption keys of data in transit to the cloud or data at rest in the service provider's data center is critical to protecting data privacy and complying with compliance mandates. The encryption of mobile media and the ability to securely share those encryption keys between the cloud service provider and consumer is an important and often overlooked need. Because moving large volumes of data quickly and cheaply over the Internet is still not practical in many situations, many organizations must send mobile media, such as an archive tape, to the cloud provider. It is critical that the data is encrypted and only the cloud provider and consumer have access to the encryption keys.

Significant restrictions regarding data co-location can arise with cloud computing, depending on an organization's location, the type of data it handles, and the nature of its business. Several member states of the European Union (EU), for example, expressly forbid the nonpublic personal information of its citizens to leave their borders.

Additionally, a cloud deployment can raise export-law violation issues relative to encrypted information, and the deployment can potentially expose intellectual property to serious threats. The organization's legal counsel must perform a thorough review of all these requirements prior to cloud deployment, making sure the organization can maintain control over the geographic location of data in the provider infrastructure.

In areas involving users and data with different risk classes that are explicitly identified (such as public and financial services), organizations need to maintain cloud-wide data classification. The classification of the data will govern who has access, how that data is encrypted and archived, and how technologies are used to prevent data loss.



Footer Field

IBM

Application and Process

Customers require **secure cloud applications** and **provider processes.**

IBM Security Framework

Establish application and environment provisioning

- Implement a program for application and image provisioning.
- A secure application testing program should be implemented.
- Ensure all changes to virtual images and applications are logged.
- Develop all Web based applications using secure coding guidelines.

IBM Cloud Security Guidance Document

Supporting IBM Products, Services and Solutions

IBM WebSphere CloudBurst Appliance
Secure cloud application deployments
Easily, securely and repeatedly create application environments, deployed and managed in a cloud

IBM Security Products and Services

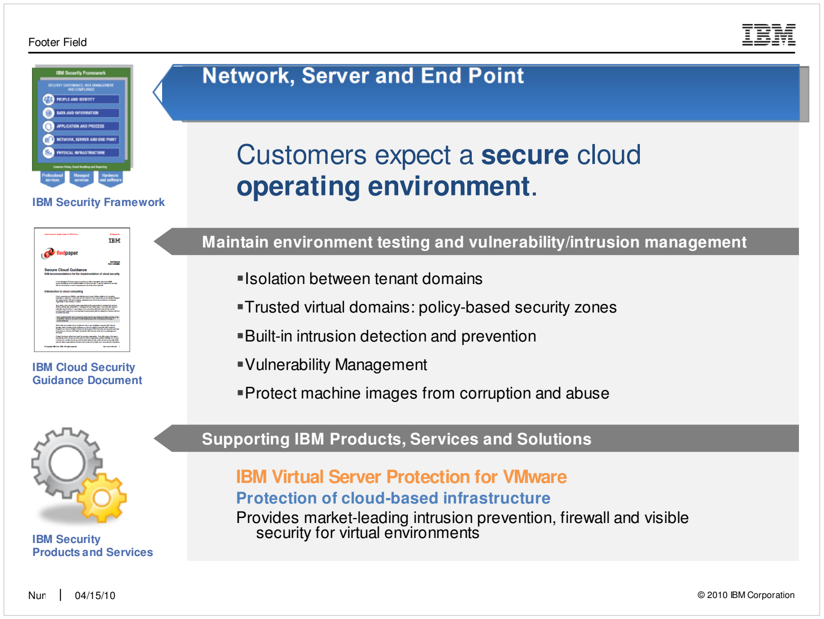
Nur | 04/15/10

© 2010 IBM Corporation

Key Point: Clients typically consider cloud application security requirements in terms of image security.

All of the typical application security requirements still apply to the applications in the cloud, but they also carry over to the images that host those applications. The cloud provider needs to follow and support a secure development process. In addition, cloud users demand support for image provenance and for licensing and usage control. Suspension and destruction of images must be performed carefully, ensuring that sensitive data contained in those images is not exposed.

Defining, verifying, and maintaining the security posture of images in regards to client-specific security policies is an important requirement, especially in highly regulated industries. Organizations need to ensure that the Web services they publish into the cloud are secure, compliant, and meet their business policies. Leveraging secure-development best practices is a key requirement.



Footer Field

IBM

Network, Server and End Point

IBM Security Framework

Customers expect a **secure** cloud **operating environment**.

IBM Cloud Security Guidance Document

Maintain environment testing and vulnerability/intrusion management

- Isolation between tenant domains
- Trusted virtual domains: policy-based security zones
- Built-in intrusion detection and prevention
- Vulnerability Management
- Protect machine images from corruption and abuse

IBM Security Products and Services

Supporting IBM Products, Services and Solutions

IBM Virtual Server Protection for VMware

Protection of cloud-based infrastructure

Provides market-leading intrusion prevention, firewall and visible security for virtual environments

Nur | 04/15/10

© 2010 IBM Corporation

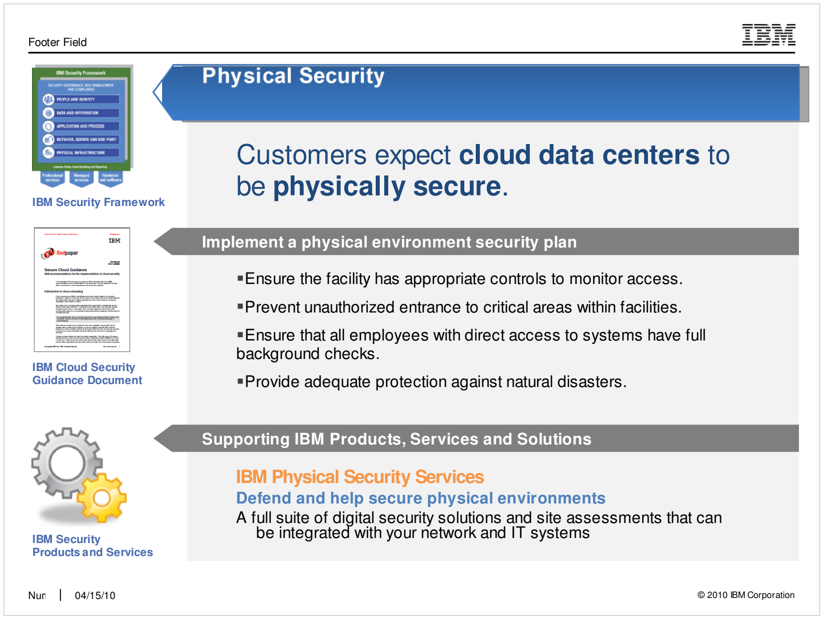
Key Point: In the shared cloud environment, clients want to ensure that all tenant domains are properly isolated and that no possibility exists for data or transactions to leak from one tenant domain into the next.

To help achieve this, clients need the ability to configure trusted virtual domains or policy-based security zones.

As data moves further from the client's control, they expect capabilities like Intrusion Detection and Prevention systems to be built into the environment. The concern is not only intrusions into a client's trusted virtual domain, but also the potential for data leakages and for *extrusions, that is, the misuse of a client's domain to mount attacks on third parties. Moving* data to external service providers raises additional concerns about internal and Internet-based denial of service (DoS) or distributed denial of service (DDoS) attacks.

In a shared environment, all parties must agree on their responsibilities to review data and perform these reviews on a regular basis. The organization must take the lead in terms of contract management for any risk assessments or controls deployment that it does not perform directly.

Where image catalogs are provided by the cloud provider, clients want these images to be secure and properly protected from corruption and abuse. Many clients expect these images to be cryptographically certified and protected.



Footer Field

IBM

Physical Security

IBM Security Framework

Customers expect **cloud data centers** to be **physically secure**.

Implement a physical environment security plan

- Ensure the facility has appropriate controls to monitor access.
- Prevent unauthorized entrance to critical areas within facilities.
- Ensure that all employees with direct access to systems have full background checks.
- Provide adequate protection against natural disasters.

IBM Cloud Security Guidance Document

Supporting IBM Products, Services and Solutions

IBM Physical Security Services

Defend and help secure physical environments

A full suite of digital security solutions and site assessments that can be integrated with your network and IT systems

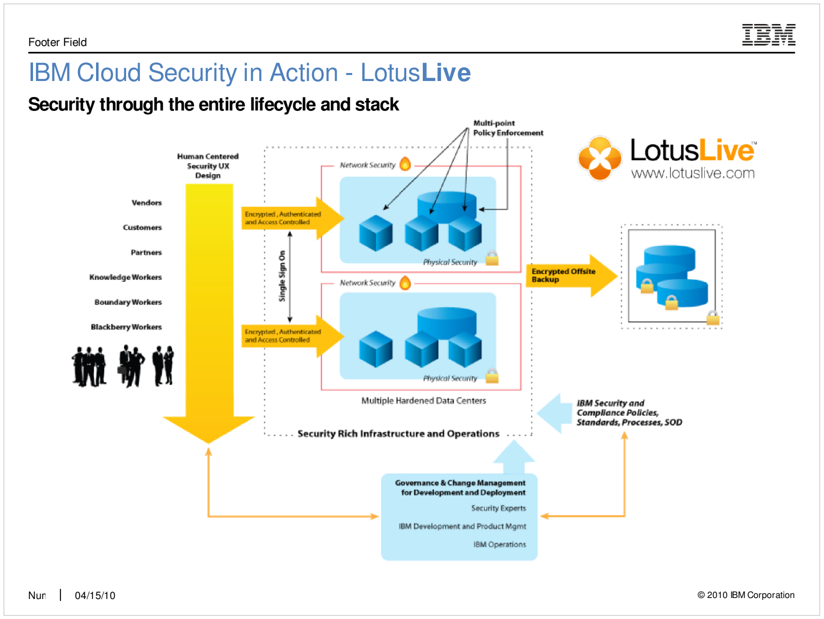
IBM Security Products and Services

Nur | 04/15/10

© 2010 IBM Corporation

Key Point: And finally, the cloud's infrastructure, including servers, routers, storage devices, power supplies, and other components that support operations, should be physically secure.

Safeguards include the adequate control and monitoring of physical access using biometric access control measures and closed circuit television (CCTV) monitoring. Providers need to clearly explain how physical access is managed to the servers that host client workloads and that support client data.



Footer Field

IBM

IBM Cloud Security in Action - LotusLive

Security through the entire lifecycle and stack

LotusLive™
www.lotuslive.com

Human Centered Security UX Design

Vendors
Customers
Partners
Knowledge Workers
Boundary Workers
Blackberry Workers

Multi-point Policy Enforcement

Network Security

Encrypted , Authenticated and Access Controlled

Physical Security

Single Sign On

Network Security

Encrypted , Authenticated and Access Controlled

Physical Security

Multiple Hardened Data Centers

Security Rich Infrastructure and Operations

Encrypted Offsite Backup

IBM Security and Compliance Policies, Standards, Processes, SOD

Governance & Change Management for Development and Deployment
Security Experts
IBM Development and Product Mgmt
IBM Operations

Nur | 04/15/10

© 2010 IBM Corporation

Enterprise Service Delivery - IBM has Deployed its Services with High Availability Enterprise Class Data Centers, High Performance Network Services and Operational Capabilities

The IBM delivery centers have deployed state of the art security and access control features Includes environmental controls such as:

•Efficient cooling systems

•Biometric cage controls

•Closed circuit TV

•Physical monitoring

•Environmental security solutions

•Utilizes a layered high availability firewall infrastructure to isolate and secure data.

•Deployed network intrusion detection and prevention infrastructure.

•Includes security event correlation and integration

Information Protection Services

•LotusLive leverages IBM's Information Protection Services (formerly Arsenal Digital) to provide robust data and systems backup and recovery capabilities.

•All backup data is encrypted

•All client communications are encrypted

•Real Time Antivirus support services with on demand scanning capabilities for the LotusLive environment.

•Single Sign on Capabilities reduce user overhead

•Leverages widely utilized Tivoli Access Manager software to provide single sign on capabilities across LotusLive components

Human Centered Security

Anti spam/anti virus features

•Outbound spam filtering

•Deactivation may be automatic based on feedback loop complaints, analysis of outbound traffic patterns, etc.

•Manually deactivates several accounts based on an evaluation of received complaints

•End user AS/AV controls - Whitelist and blacklist controls, junk mail folders, user feedback loops

•Javascript filtering from email

•Disabling of image display

Footer Field

Trusted Advisor

Solution Provider

Security Company

The Company

Security for the Cloud

Security & Privacy Leadership

Nur | 04/15/10

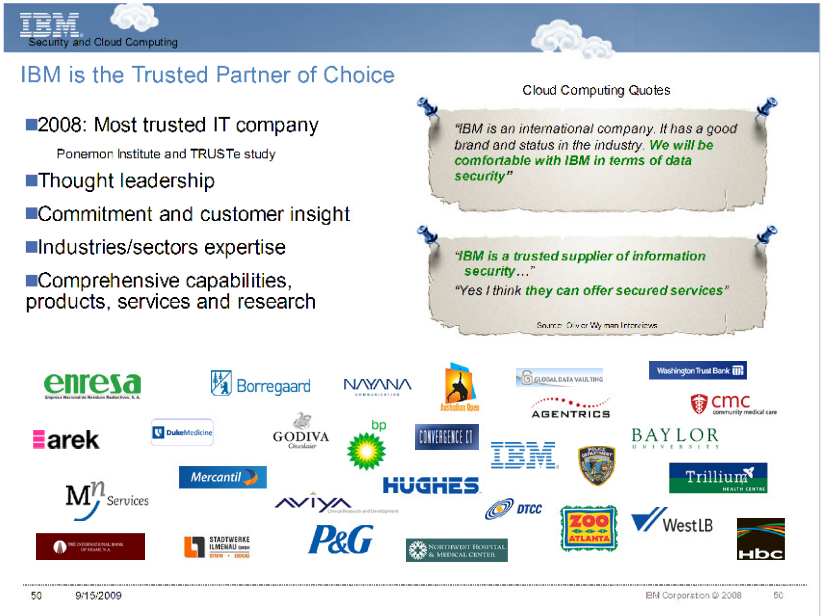
© 2010 IBM Corporation

[Self-explanatory]

IBM Security: Sum is greater than its parts!

SC MAGAZINE AWARDS 2010 WINNER
Honored in the U.S.

On Tuesday March 2, IBM Corporation was named "Best Security Company" for 2010 by SC Magazine, recognizing IBM's outstanding achievement in risk management and its comprehensive family of security solutions. As the industry's preeminent awards program, the annual SC Awards has recognized security's key contributors and outstanding products for more than a decade.



IBM is the Trusted Partner of Choice

- 2008: Most trusted IT company

  Ponemon Institute and TRUSTe study
- Thought leadership
- Commitment and customer insight
- Industries/sectors expertise
- Comprehensive capabilities, products, services and research

Cloud Computing Quotes

> *"IBM is an international company. It has a good brand and status in the industry.* ***We will be comfortable with IBM in terms of data security"***

> ***"IBM is a trusted supplier of information security…"***
>
> *"Yes I think* ***they can offer secured services"***

Source: Oliver Wyman Interviews

Thank you!

For more information, please visit:
ibm.com/cloud
Ibm.com/security

© 2010 IBM Corporation

Backup slides

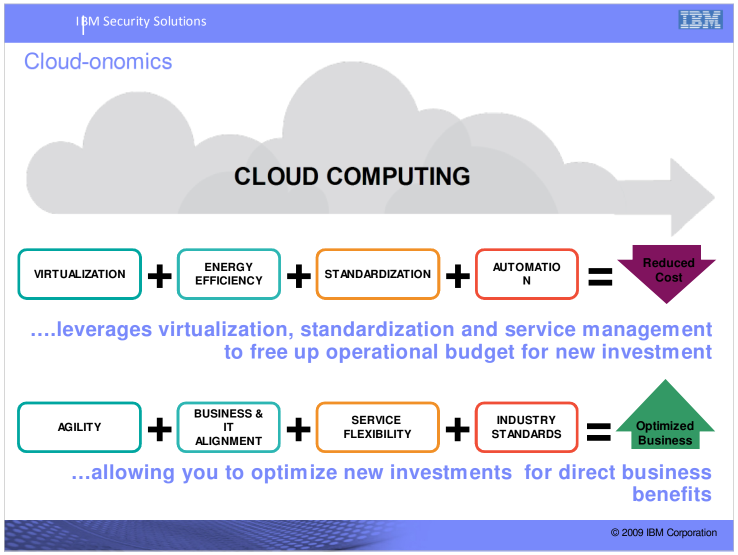
© 2010 IBM Corporation

Cloud Computing and Virtualization: New Challenges for Security Management

January 2010

Scott Henley
IBM Security Solutions
scott.henley@au1.ibm.com

© 2010 IBM Corporation



IBM Security Solutions

Cloud-onomics

CLOUD COMPUTING

VIRTUALIZATION + ENERGY EFFICIENCY + STANDARDIZATION + AUTOMATIO N = Reduced Cost

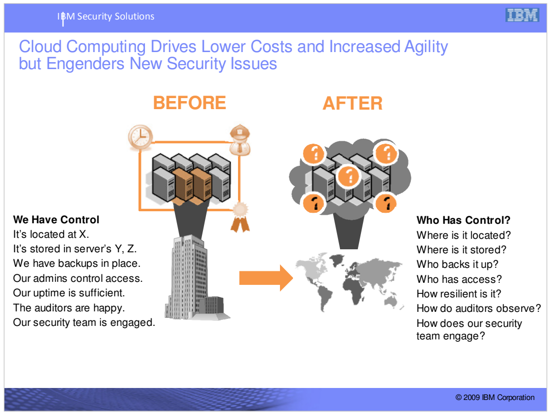
....leverages virtualization, standardization and service management to free up operational budget for new investment

AGILITY + BUSINESS & IT ALIGNMENT + SERVICE FLEXIBILITY + INDUSTRY STANDARDS = Optimized Business

...allowing you to optimize new investments for direct business benefits

© 2009 IBM Corporation

Image from Microsoft Clip Art



IBM Security Solutions

Cloud Computing Drives Lower Costs and Increased Agility but Engenders New Security Issues

BEFORE

AFTER

We Have Control
It’s located at X.
It’s stored in server’s Y, Z.
We have backups in place.
Our admins control access.
Our uptime is sufficient.
The auditors are happy.
Our security team is engaged.

Who Has Control?
Where is it located?
Where is it stored?
Who backs it up?
Who has access?
How resilient is it?
How do auditors observe?
How does our security team engage?

© 2009 IBM Corporation

Virtualization enables businesses to compete effectively and efficiently

Facilitate Physical Consolidation

- Manage server sprawl
- Improve utilization
- Reduce costs
- Lower power usage

Achieve High Performance

- Rapid application deployment
- Share resources optimally
- Automate workload management
- Enables high availability

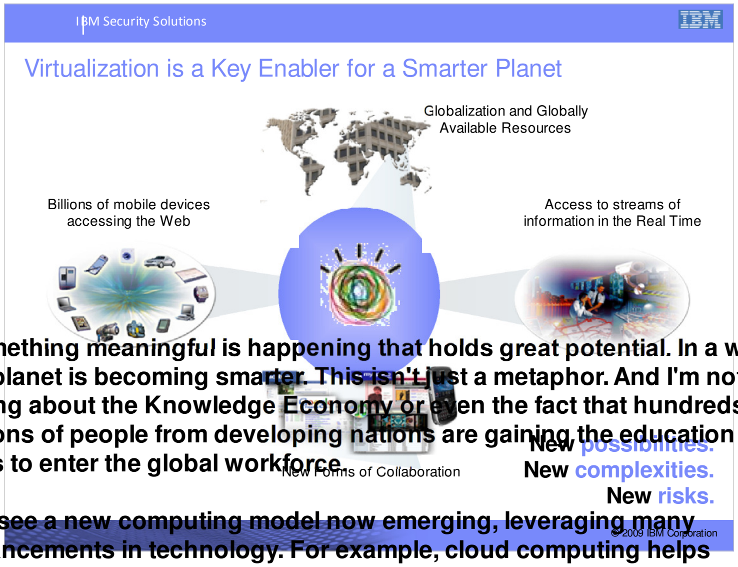
Improve Service Levels

- Increase service reliability
- Simplify backup and recovery
- Bring new services online quickly

Enable Cloud Computing

- Always available
- Easily expandable
- Automated provisioning
- Simplified user experience

© 2009 IBM Corporation



IBM Security Solutions

Virtualization is a Key Enabler for a Smarter Planet

Globalization and Globally Available Resources
Billions of mobile devices accessing the Web
Access to streams of information in the Real Time
New Forms of Collaboration

New possibilities.
New complexities.
New risks.

© 2009 IBM Corporation

•Something meaningful is happening that holds great potential. In a word, our planet is becoming smarter. This isn't just a metaphor. And I'm not talking about the Knowledge Economy or even the fact that hundreds of millions of people from developing nations are gaining the education and skills to enter the global workforce.

•We see a new computing model now emerging, leveraging many advancements in technology. For example, cloud computing helps address the demand for ubiquitous access of information driven by the maturing role of the Mobile Web, the rise of social networking, globalization and the availability of global resources as well as the onset of real time data streaming and access to information. These are all becoming interconnected phenomena and the advancements in technology are driving this at breakneck speed.

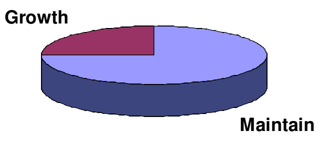
•In today’s business environment, the only constant is change and it takes a dynamic infrastructure to allow an organization to adapt quickly. To be dynamic that means to:

1.Improve Service: To respond to opportunities and challenges with agility and speed, an organization must have business-driven service management model that scales dynamically and provides superior visibility, control, and automation of the business and IT infrastructure, including the proliferation of mobile and connected devices.
2.Reduce Cost: Mounting economic pressures, global competition, shifting consumer demands, and the emergence of new technology combine to place increasing pressure on businesses to move faster, yet resources are limited with costs and complexity increasing. A new model must be employed that allows the organization to be more efficient.
3.Manage Risk: The explosion of information, devices, and things connected to the network combined with the growing inter-connectedness of people and processes generates new business and operational risks. Business and IT security and resiliency are as critical as ever, and must be dynamic and intelligent in order to match the speed of business change.

Transition: **So what type of risks are we talking about?**

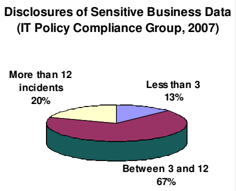
Managing Risks Introduced by New Opportunities

Complexity of Infrastructure



% of IT Investment Spent on Maintaining Existing Infrastructure

Explosion of Data



Disclosures of Sensitive Business Data

Sources: IBM; IT Policy Compliance Group

© 2009 IBM Corporation

Virtualization has many benefits but introduces new complexities

- Virtualization blurs the physical boundaries between systems that are used to separate workloads and those responsible for securing them.
- Virtualization enables mobility of systems and flexible deployment and re-deployment of systems. Manually tracking software stacks and configurations of VMs and images becomes increasingly difficult.

Before Virtualization

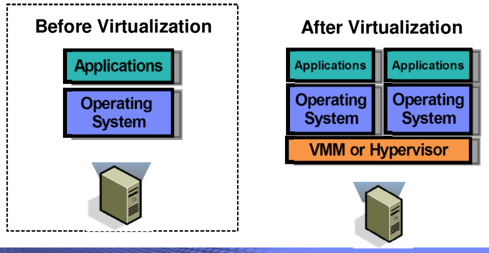
After Virtualization

© 2009 IBM Corporation

Virtualization has many benefits but introduces new complexities

- Virtualization blurs the physical boundaries between systems that are used to separate workloads and those responsible for securing them.

- Virtualization enables mobility of systems and flexible deployment and re-deployment of systems. Manually tracking software stacks and configurations of VMs and images becomes increasingly difficult.



Before Virtualization

Applications

Operating System

After Virtualization

Applications

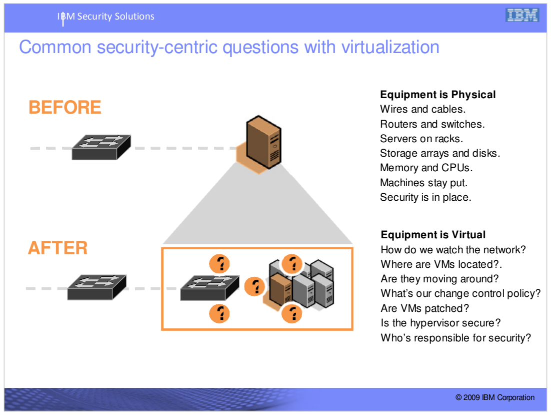
Applications

Operating System

Operating System

VMM or Hypervisor

© 2009 IBM Corporation



IBM Security Solutions

Common security-centric questions with virtualization

BEFORE

AFTER

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.

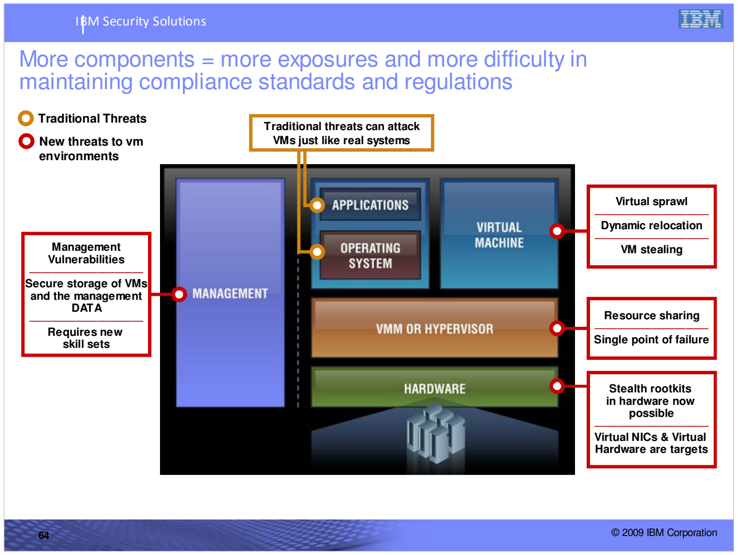
Equipment is Virtual
How do we watch the network?
Where are VMs located?.
Are they moving around?
What's our change control policy?
Are VMs patched?
Is the hypervisor secure?
Who's responsible for security?

© 2009 IBM Corporation

Common security-centric concerns with virtualization

	Physical Network	Virtual Security
Network IPS	Block threats & attacks at perimeter and between network segments	Block threats & attacks on virtual network segments
Server Protection	Secure each physical server with multi-layered protection & reporting on a single agent	Securing each VM as if it were a physical server can mean significant time and cost to system admin
System Patching	Patch critical vulnerabilities on each server and network	Dynamic environments lead to un-patched VMs; Difficult to track VM sprawl and keep VMs patched
Security Policies	Set policies specific to critical applications in each network segment & server	Virtualization often drives variety of OS and apps on a single server, so security policies must be more encompassing – web, data, OS coverage, databases, etc.
Integrate Security w/ Virt. Infrastructure	NA	*New frontier of risk requires dedicated features to protect the hypervisor & assist in VM management*

© 2009 IBM Corporation



More components = more exposures and more difficulty in maintaining compliance standards and regulations

○ Traditional Threats

○ New threats to vm environments

Traditional threats can attack VMs just like real systems

APPLICATIONS

OPERATING SYSTEM

VIRTUAL MACHINE

MANAGEMENT

VMM OR HYPERVISOR

HARDWARE

Management Vulnerabilities

Secure storage of VMs and the management DATA

Requires new skill sets

Virtual sprawl

Dynamic relocation

VM stealing

Resource sharing

Single point of failure

Stealth rootkits in hardware now possible

Virtual NICs & Virtual Hardware are targets

© 2009 IBM Corporation

Current best practices for securing virtualization through compliance-oriented internal controls

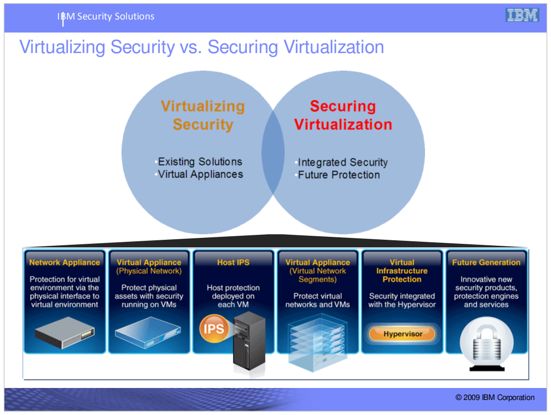
1. Harden platforms to reduce the risk unauthorized access
2. Configuration and change management processes should be extended to encompass the virtual infrastructure
   - Can add cost and complexity for system administrator to continuously reconfigure in a dynamic environment
   - Ensure patch management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

Source: RSA Security Brief: Security Compliance in a Virtual World

http://w w w .rsa.com/solutions/technology/secure/w p/10393_VIRT_BRF_0809.pdf

© 2009 IBM Corporation

Virtualizing Security vs. Securing Virtualization



Virtualizing Security

- Existing Solutions
- Virtual Appliances

Securing Virtualization

- Integrated Security
- Future Protection

Network Appliance

Protection for virtual environment via the physical interface to virtual environment

Virtual Appliance (Physical Network)

Protect physical assets with security running on VMs

Host IPS

Host protection deployed on each VM

Virtual Appliance (Virtual Network Segments)

Protect virtual networks and VMs

Virtual Infrastructure Protection

Security integrated with the Hypervisor

Future Generation

Innovative new security products, protection engines and services

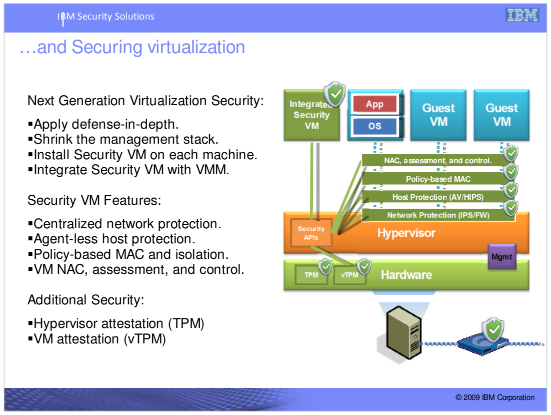
© 2009 IBM Corporation

Virtualizing Security…
IBM Proventia Virtualized Network Security Platform

- Market-leading network protection now available on VMWare virtual platform
  - World class, vulnerability-based protection powered by X-force research
  - "Virtual appliance"
- Protection for virtual environments
  - Intrusion prevention and network protection for traffic between vSwitches
  - Protect the virtual machines on a server
- Integrate and manage virtual security with traditional network security
  - Single management console

Virtual Security Appliances

© 2009 IBM Corporation



…and Securing virtualization

Next Generation Virtualization Security:

- Apply defense-in-depth.
- Shrink the management stack.
- Install Security VM on each machine.
- Integrate Security VM with VMM.

Security VM Features:

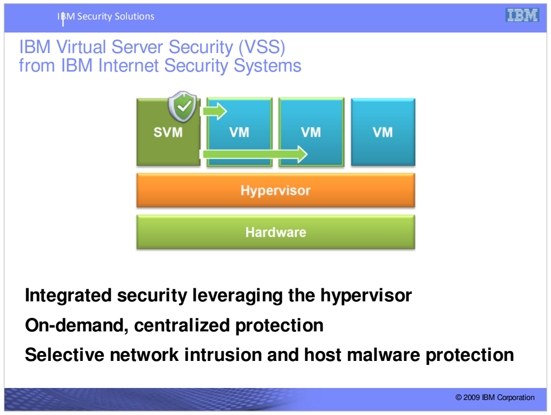
- Centralized network protection.
- Agent-less host protection.
- Policy-based MAC and isolation.
- VM NAC, assessment, and control.

Additional Security:

- Hypervisor attestation (TPM)
- VM attestation (vTPM)

© 2009 IBM Corporation

IBM Virtual Server Security (VSS) from IBM Internet Security Systems

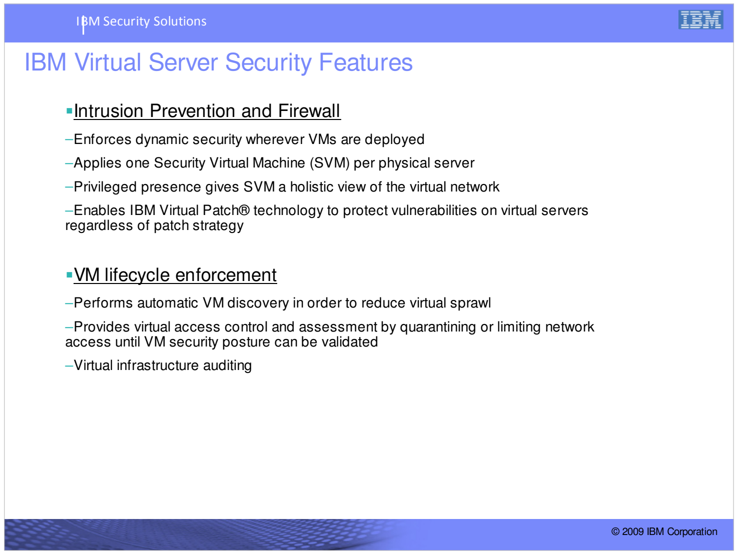


Integrated security leveraging the hypervisor

On-demand, centralized protection

Selective network intrusion and host malware protection

© 2009 IBM Corporation



IBM Virtual Server Security Features

- 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

© 2009 IBM Corporation

IBM Security Solutions for Cloud Computing

1 Cloud Security Consulting

IBM Strategy Mapping:

Define, invest in, and develop Cloud Consulting Services

Offer IBM ISS professional security services to clients engaging in cloud initiatives.

Examples:

- Cloud assessment services
- Penetration testing for the Cloud
- Information security assessment

2 Cloud Security Products

Technologies in support of cloud computing

IBM Strategy Mapping:

Develop a Standardized Cloud Implementation methodology with supporting technologies

Develop products and technologies to protect cloud infrastructures and their tenants.

Examples:

- Proventia Network IPS and Virtual IPS appliances
- Virtual Server Security for VMware
- Identity and access management
- Security event and information management

3 Cloud-based Security Services

Smart business Security Services

IBM Strategy Mapping:

Develop and extend selected ITS Managed Services offerings

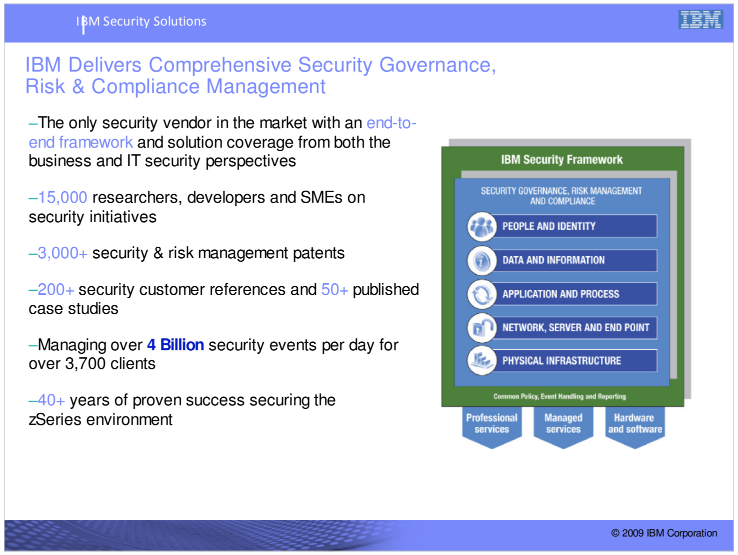
Leverage the cloud as a delivery mechanism for IBM security services.

Examples:

- Vuln management service
- Email scrubbing service
- Web content filtering service
- Security event log management

Securing Cloud Infrastructures → **Security from an IBM ISS Cloud**

© 2009 IBM Corporation



IBM Security Solutions

IBM Delivers Comprehensive Security Governance, Risk & Compliance Management

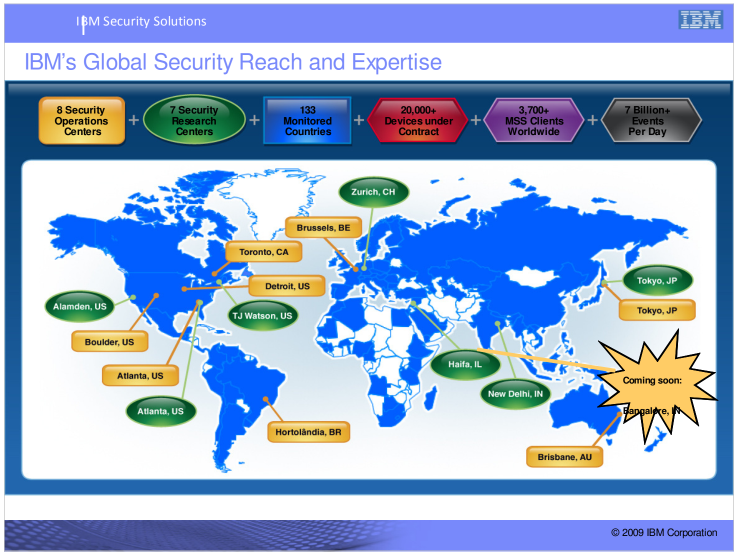
- –The only security vendor in the market with an end-to-end framework and solution coverage from both the business and IT security perspectives
- –15,000 researchers, developers and SMEs on security initiatives
- –3,000+ security & risk management patents
- –200+ security customer references and 50+ published case studies
- –Managing over **4 Billion** security events per day for over 3,700 clients
- –40+ years of proven success securing the zSeries environment

© 2009 IBM Corporation

•IBM's approach is to strategically manage risk end-to-end across all five domains of IT security.

•The multi-dimension aspect of the framework is supported by IBM’s thousands of research professionals, hundreds of patents and a long and deep history of supporting customers.

•By rethinking IT service delivery, CIOs can move to a new, centrally governed enterprise data center model that is efficient, service oriented, locally responsive and flexible. IBM can help clients identify how to



IBM Security Solutions

IBM’s Global Security Reach and Expertise

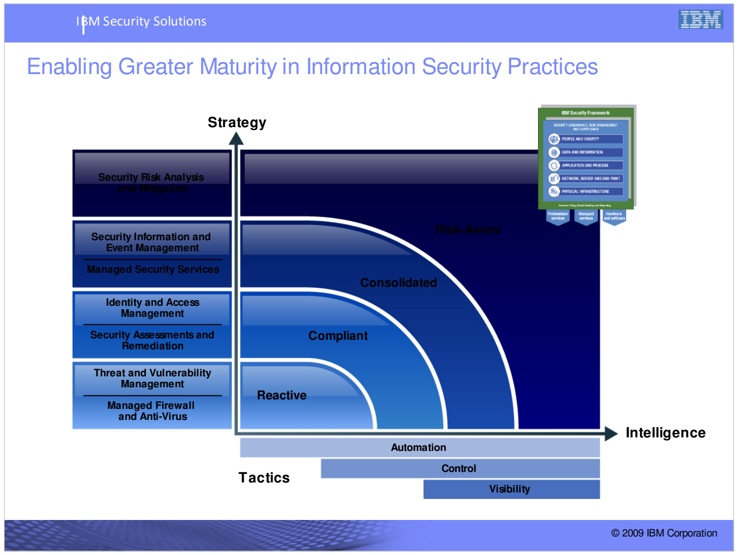
8 Security Operations Centers + 7 Security Research Centers + 133 Monitored Countries + 20,000+ Devices under Contract + 3,700+ MSS Clients Worldwide + 7 Billion+ Events Per Day

© 2009 IBM Corporation

No other vendor can match IBM’s global security reach and expertise.

IBM has eight MSS Security Operations Centers in North America, South America, Europe and Asia, monitors more than 17,000 security devices in 133 countries on behalf of 3,700 customers. Customers range from Small and Medium businesses to some of the largest corporations and government organizations in the world. IBM serves clients in all industries. This global reach allows us to serve clients with international capabilities and a local presence.

IBM MSS analyses more than 2.5 billion security events every single day giving us unparalleled access to real-time threat and vulnerability information that benefits our clients as a whole and allows us to provide protection ahead of the threat.



IBM Security Solutions

Enabling Greater Maturity in Information Security Practices

Strategy

Security Risk Analysis and Mitigation

Security Information and Event Management

Managed Security Services

Identity and Access Management

Security Assessments and Remediation

Threat and Vulnerability Management

Managed Firewall and Anti-Virus

Risk-Aware

Consolidated

Compliant

Reactive

Intelligence

Tactics

Automation

Control

Visibility

© 2009 IBM Corporation

The concept here is that Tivoli offers every conceivable product, to solve every conceivable pain. The trick is to ensure that as you start down the automation path, you want to make sure that those tools can be integrated within an “intelligent design”.

For More Information: IBM Virtualization Security Solutions

Virtualization Security Solutions Webpage

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

Home | Solutions | Services | Products | Support & downloads | My IBM
Welcome Mrs. Dori White [Not you?] [IBM Sign in]

Virtualization Security Solutions from IBM Internet Security Systems™

Manage the risks of virtualization and realize the cost savings

Overview | Virtual environment ready solutions | Virtual appliances | Virtual infrastructure protection | Virtualization security management

What we offer

IBM ISS brings comprehensive, end-to-end security to virtualization, enabling you to more quickly realize the benefits of virtualization technology with:

- Virtual environment ready solutions
- Virtual appliances
- Virtual infrastructure protection
- Virtualization security management

Virtualization security the right way

While there are many virtualization security options, it is critical to understand that the true value of security is not in point products that

We're here to help

Easy ways to get the answers you need.

or call us at
1-800-IBM-7080
Mention 108AE08W

Virtualization White Paper
June 2009

Securing Virtualization in Real-World Environments
IBM Internet Security Systems

White Paper

Links work in presentation mode

© 2010 IBM Corporation

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

White paper link: ftp://ftp.software.ibm.com/common/ssi/sa/wh/n/sew03016usen/SEW03016USEN.PDF

Thank
You