Securing Virtualization in real World Environments

Sukhdev Singh IBM ASEAN

CISSP

CISM

XFE

Certified Enterprise Architect (TOGAF®)

Pulse2010

The Premier Service Management Event

Agenda

- Components of Cloud Market
- Basic Security Concepts – Today and tomorrow
- IBM’s vision of a Security Framework
- IBM Cloud Security Guidance
- Conceptual findings from Security Framework
- IBM products to achieve actual security results

Impact of cyber security is becoming more apparent…

$226 Billion

Economic impact of cyber attacks on businesses has grown to over $226 billion annually.

Source: Congressional Research Service study

158% increase

Security breaches are on the increase: cyber attacks have increased 158% since 2006[1],

Sources: [1]US Department of Homeland Security,

52%

Private-sector statistics show that the insider threat is up more than 52% in the past year.

Exposing sensitive personal information means always having to say you're sorry. Some

Data Breach at Radisson Hotels, Stolen Credit Card Numbers

The hotel chain has hidden its data breach for about three months

The Radisson Hotels & Resorts chain has issued an apology letter have been accommodated in some of its Canadian and US-based data breach in the hotel's credit-card security system that allowed customer credit-card information. According to the official pres breached between November 2008 and May 2009.

After keeping it under wraps for about three months, Radisson apology to their customers and informed the media about this incide

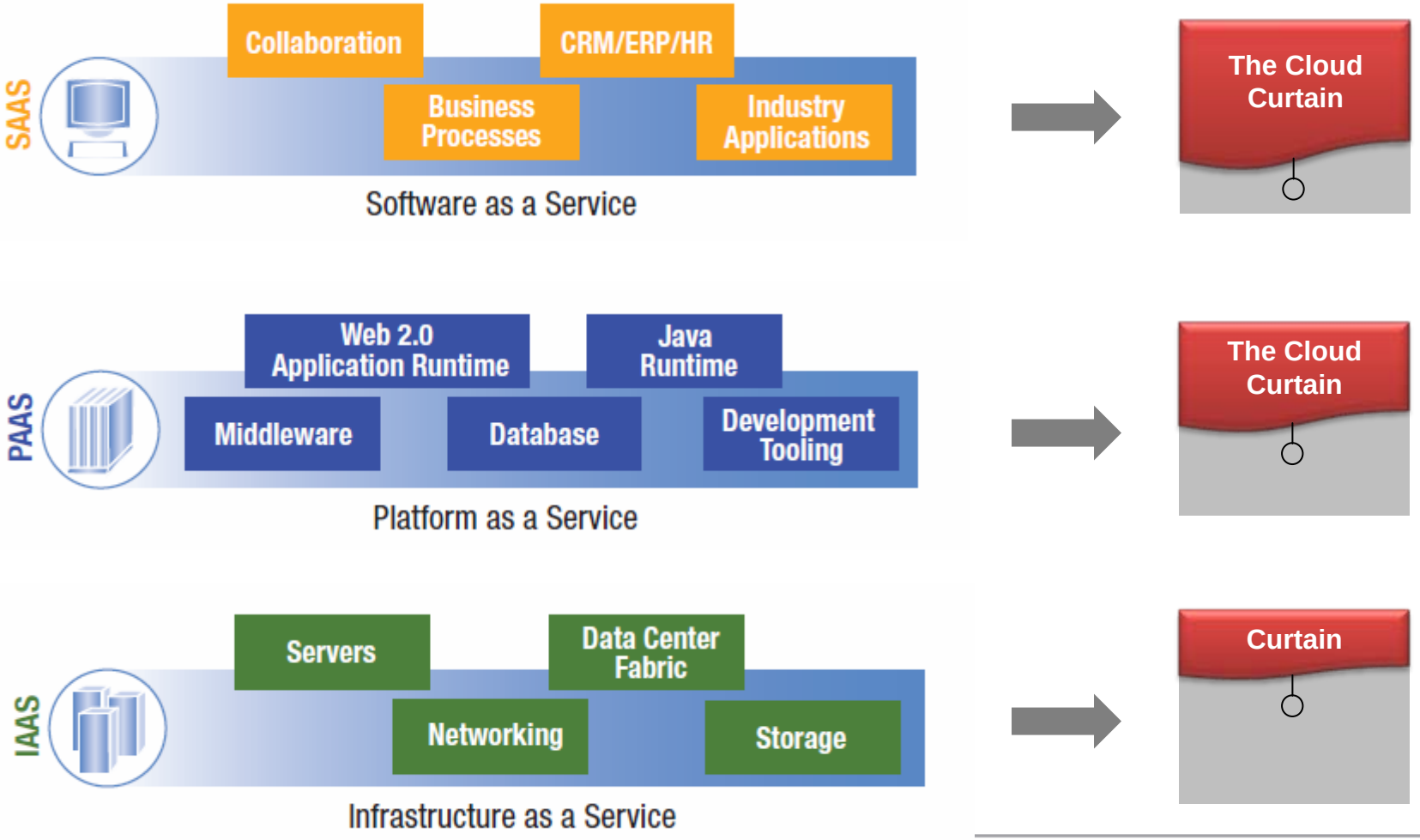
stores, warned customers in January that its computer network had been broken into in May 2006, compromising customer credit-card information and other data. TJX announced in February that an investigation showed intruders had gained access to TJX systems almost a full year earlier than initially thought and had compromised more payment card data than initially believed.

What is at Risk ?

- Interruption of business operations (Lost Revenues)
- Decreased productivity due to additional strain placed on network resources (Lost Revenues)
- Loss of confidential information (Lost Competitive Advantage)
- Increased recruiting and staffing costs (Lost Profits)

คำแปล

Cloud Model Applies at all Levels of the IT Stack – Resulting in Different Security Requirements, Different Responsibilities



What is Cloud Security?

Confidentiality, Integrity, Availability
of business-critical IT assets

Stored or processed on a cloud computing platform

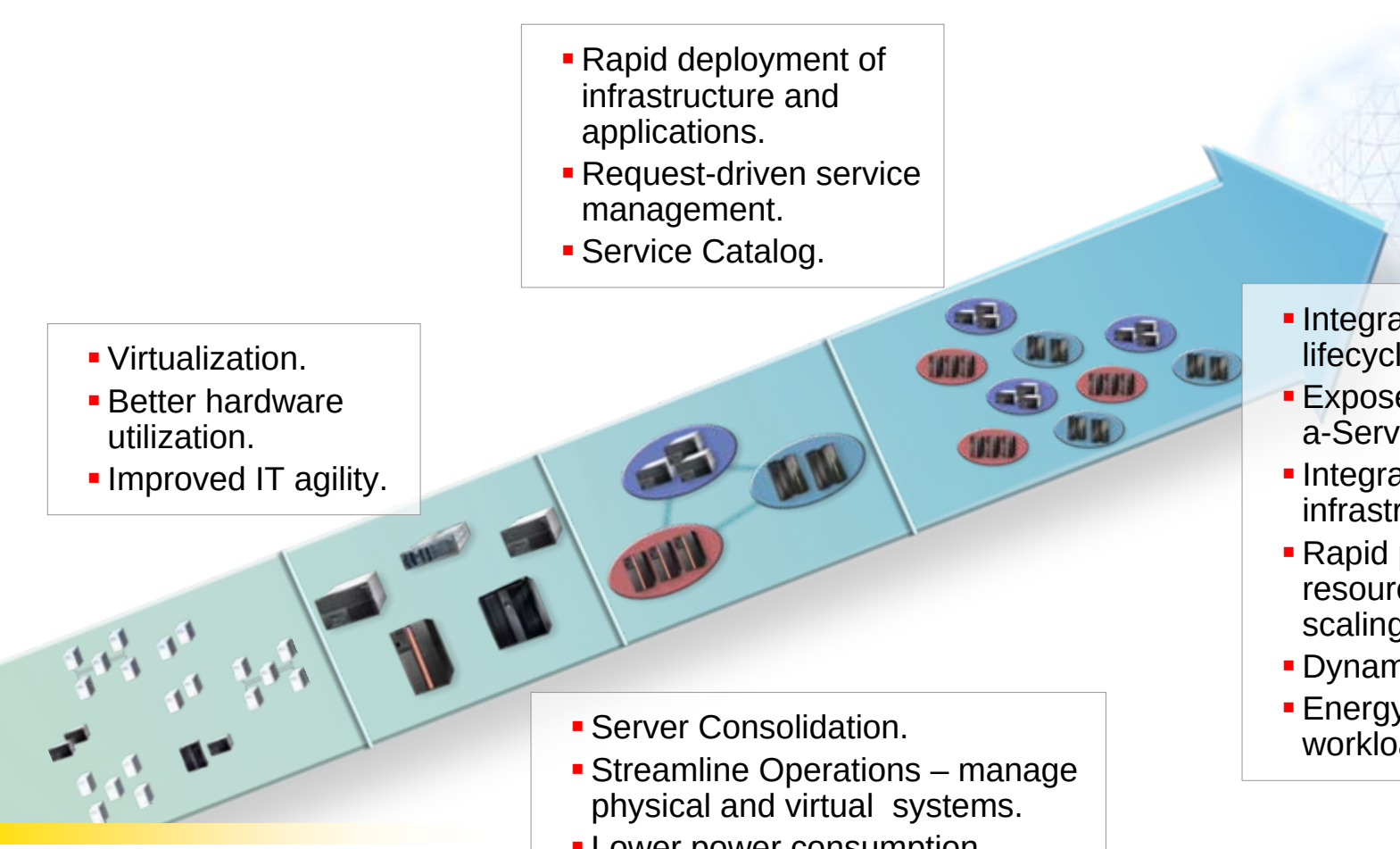
There is nothing new under the sun
but there are lots of old things we don't know.

Ambrose Bierce, The Devil's Dictionary

Virtualization – First Step in Journey to Cloud Computing

- Virtualization.
- Better hardware utilization.
- Improved IT agility.

- Rapid deployment of infrastructure and applications.
- Request-driven service management.
- Service Catalog.



Cloud Computing

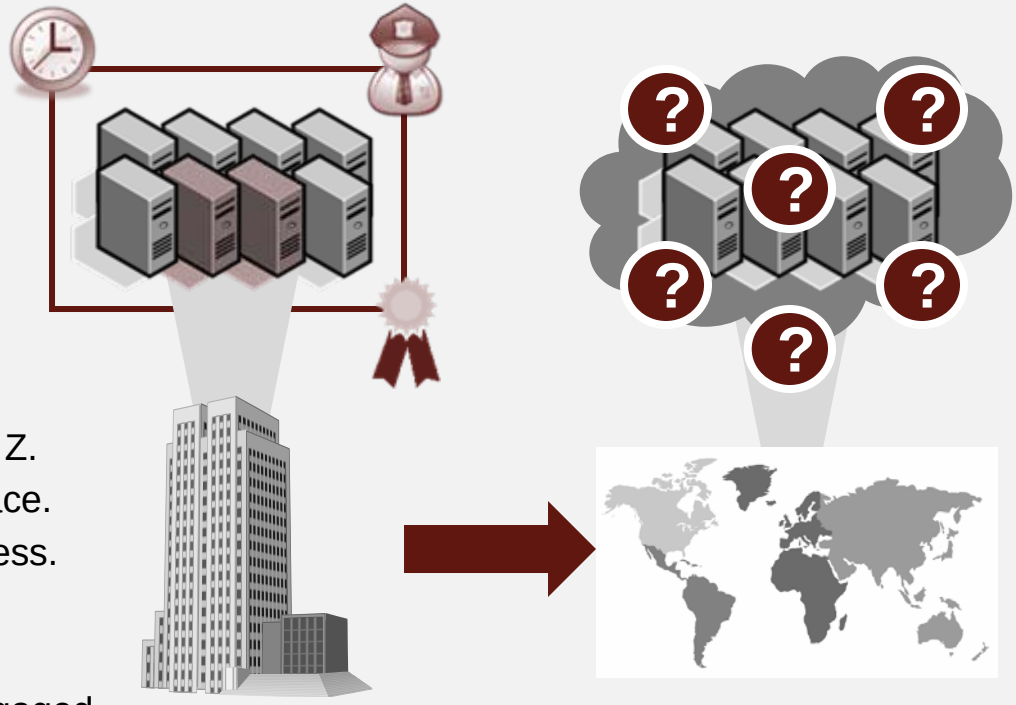
- Integrated service lifecycle mgmt.
- Expose resources “as-a-Service”.
- Integrated Security infrastructure.
- Rapid provisioning of IT resources, massive scaling.
- Dynamic service mgmt.
- Energy saving via auto workload distribution.

- Server Consolidation.
- Streamline Operations – manage physical and virtual systems.
- Lower power consumption.

Cloud Security: 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?

IBM Security Solutions

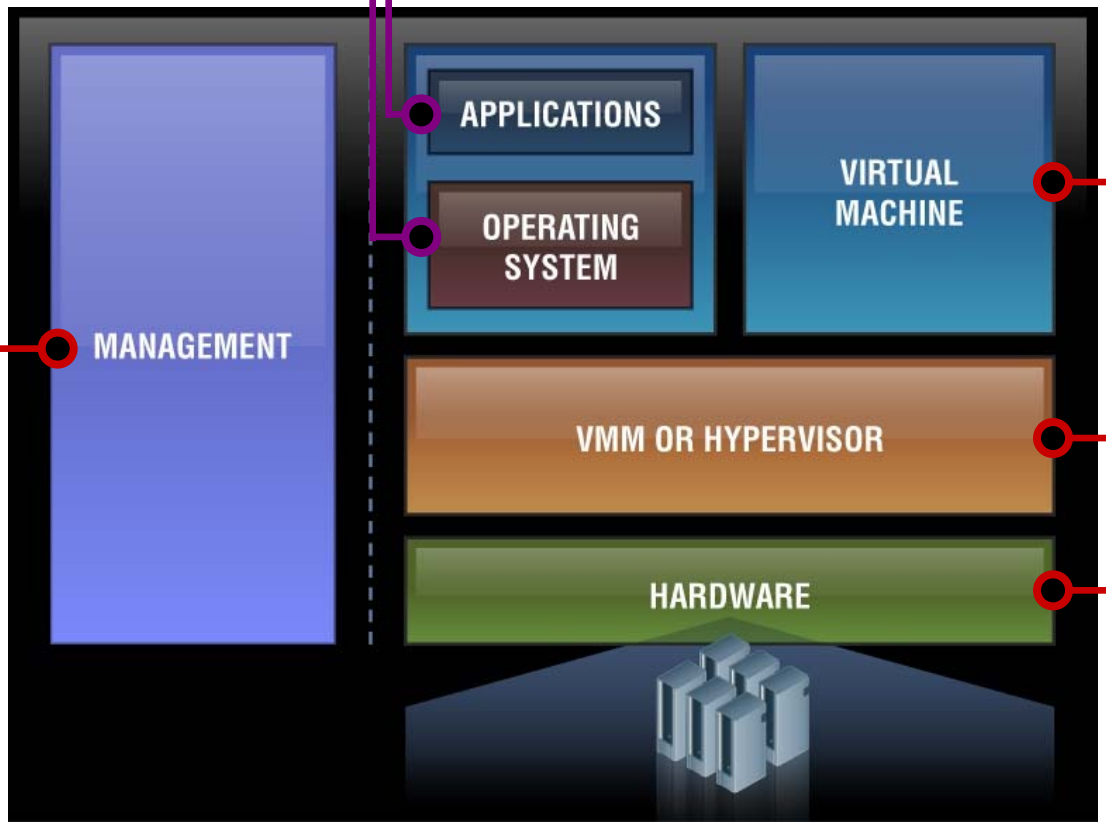
X-Force® 2009 Trend and Risk Report:

Annual Review of 2009

More Components = More Exposure

- 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

Image from Microsoft Clip Art

Image from Microsoft Clip Art

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 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.

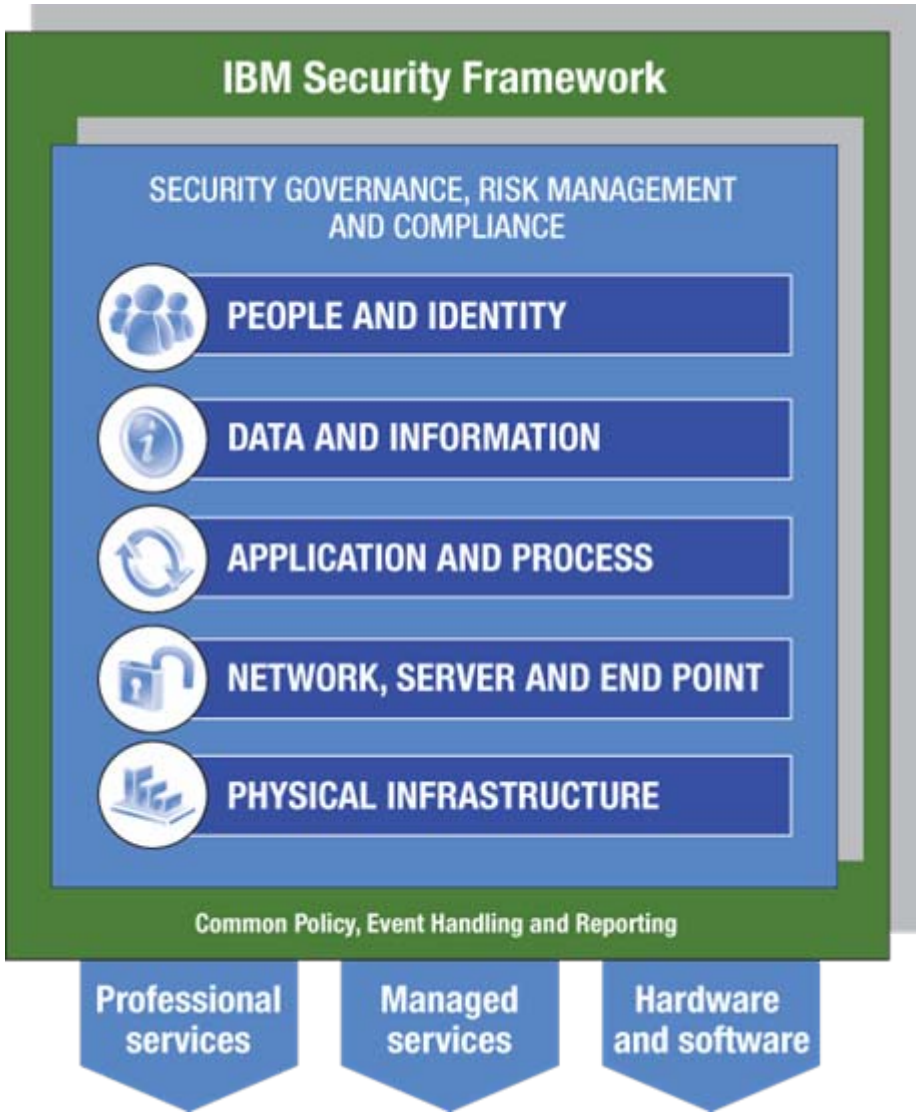
IBM Security Framework – Business-oriented framework used across all IBM brands that allows to structure and discuss a client's security concerns

Built to meet four key requirements:

- Provide *Assurance*
- Enable *Intelligence*
- Automate *Process*
- Improve *Resilience*

Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security;

IBM RedGuide REDP-4528-00, July 2009



Typical Client Security Requirements

Governance, Risk Management, Compliance

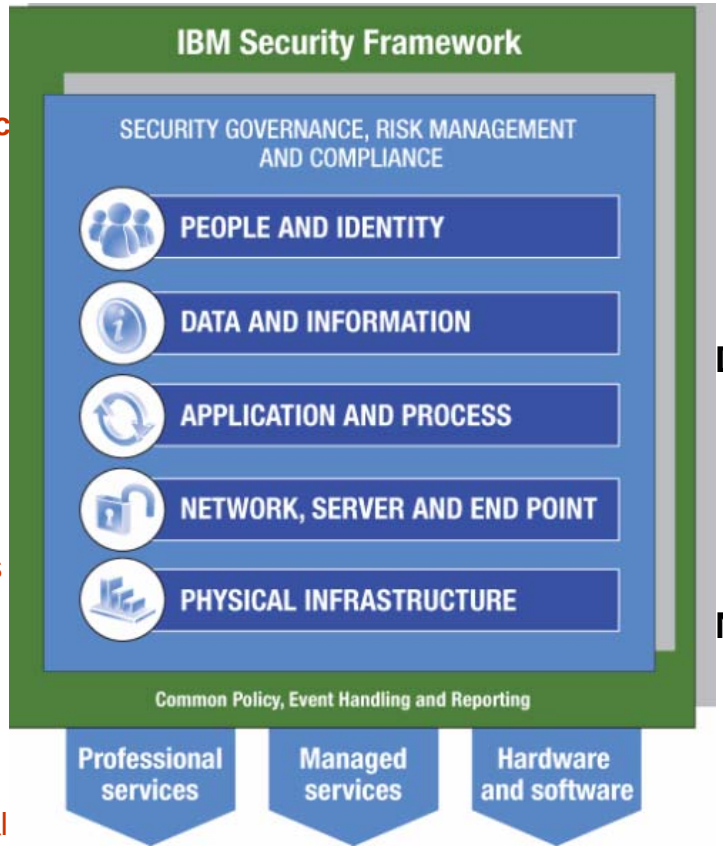
- **3rd-party audit** (SAS 70(2), ISO27001, PCI)
- **Client access to tenant-specific log and audit data**
- **Effective incident reporting for tenants**
- Visibility into change, incident, image management, etc.
- SLAs, option to transfer risk from tenant to provider
- Support for forensics
- Support for e-Discovery

Application and Process

- Application security requirements for cloud are phrased in terms of image security
- Compliance with secure development best practices

Physical

- Monitoring and control of physical access



People and Identity

- **Privileged user monitoring,** including logging activities, physical monitoring and background checking
- **Federated identity / onboarding:** Coordinating authentication and authorization with enterprise or third party systems
- **Standards-based SSO**

Data and Information

- **Data segregation**
- Client control over geographic location of data
- Government: Cloud-wide data classification

Network, Server, Endpoint

- **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
- Government: MILS-type separation

Based on interviews with clients and various analyst reports

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
- SC Security Company of the year 2010 RSA Security

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

BEST SECURITY COMPANY

WINNER
IBM Corporation
www.ibm.com/security

Founded in 1911, IBM has been a security industry leader for nearly 50 years, helping CxOs and IT professionals secure their corporate infrastructures with solutions that go beyond just collections of niche products. Customers rely on IBM for the planet's most secure databases, applications, operating systems, storage and servers.

IBM offers comprehensive security solutions and services addressing compliance, applications, data, identity and access management, networks, threat prevention, systems security, email, encryption, virtualization and cloud security.

Through an end-to-end approach to security across people and identity, data, applications, compliance, networks, servers and the physical infrastructure, IBM offers security capabilities that are among the top in the industry. With multiple leadership awards in market presence and technology innovation, IBM is able to offer more than 120 security products and the experience of over 15,000 researchers, developers and SMEs focused on security initiatives.

IBM clients around the world gain the benefit of integrated, security solutions that reduce the cost and complexity of managing security solutions from multiple vendors.

World-class security support services from IBM provide the technical and operational expertise needed to maximize security investment. By providing a global network of support centers to assist customers worldwide, often in their native language, IBM partners with its customers around the clock to solve any implementation and technical issues.

This support is available regardless of client location or implementation method of hardware, software and/or managed security services. IBM provides a variety of support levels – from self-help to tiered levels – enabling customers to choose the one that best meets their needs. IBM is recognized for its outstanding customer support and consistently high customer satisfaction.

The company has staked a firm claim in the security marketplace and emerged as a market leader capable of meeting any global organization's security needs through an integrated, diverse and flexible portfolio of products and services across key industries.

With a strong, deep and broad security portfolio, IBM is in a strong position, able to leverage its considerable assets and reputation and provide innovative technologies and intellectual property that address both today's vulnerabilities and newly emerging threats.

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

IBM Cloud Security Guidance document

- Based on cross-IBM research 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*

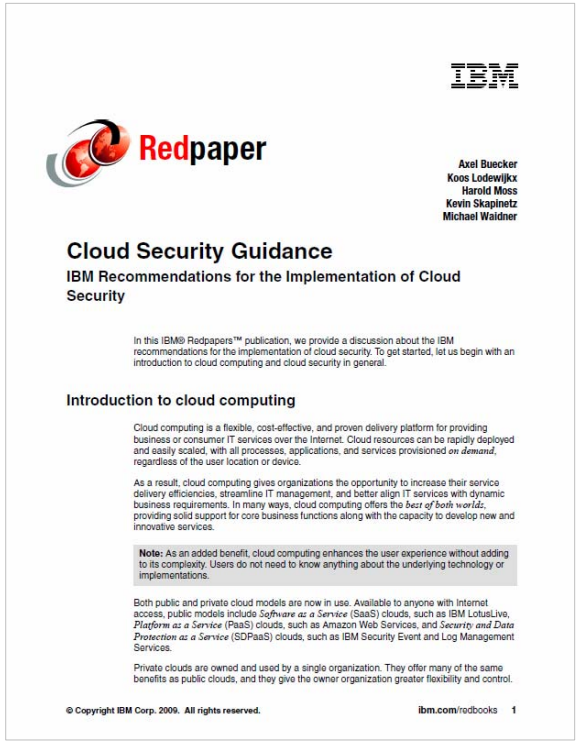
  – *Implementing Strong Access and Identity*

  – *Application Provisioning and De-provisioning*

  – *Governance Audit Management*

  – *Vulnerability Management*

  – *Testing and Validation*


IBM

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.

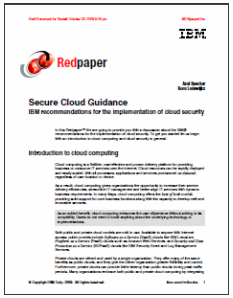
As a result, cloud computing gives organizations the opportunity to increase their service delivery efficiencies, streamline IT management, and better align IT services with dynamic business requirements. In many ways, cloud computing offers the *best of both worlds*, providing solid support for core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

IBM Security Framework



IBM Cloud Security Guidance Document

Security governance, risk management and compliance

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

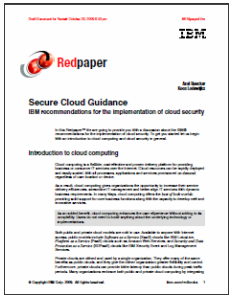
Implement a governance and audit management program

- Establish 3rd-party audits (ISO27001, PCI)
- Provide access to tenant-specific log and audit data
- Create effective incident reporting for tenants
- Visibility into change, incident, image management, etc.
- Create policies for PII and for data crossing International boundaries
- Understand applicable regional, national and international laws
- Support for forensics and e-Discovery

IBM Security Framework

People and Identity

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



IBM Cloud Security Guidance Document

Implement strong identity and access management

- Implement least privilege model for user's access
- Strong Identity lifecycle management
- All administrative access over secure channels
- 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

People and Identity

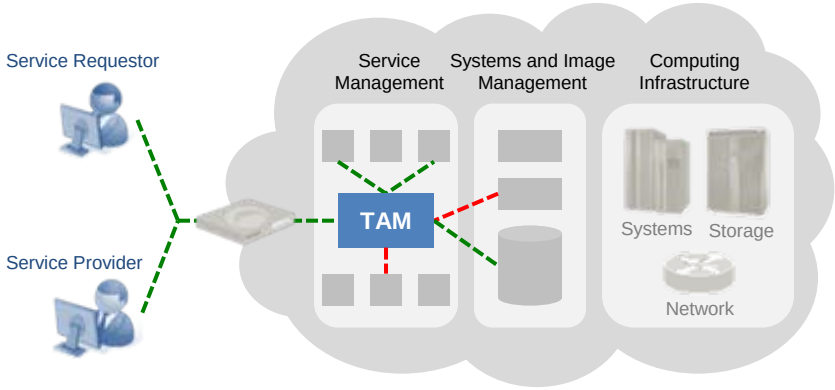
Tivoli Access Manager (TAM)

Privileged User Access

Separation of administrative and user roles in a cloud environment

Summary: Access management and single sign-on solution that manages the difficulty of executing security policies across a wide range of Web and application resources.

Cloud Use Case: Provides validation and processing of user identity information. Addresses the need of authentication of users within the cloud ecosphere. Defines and manages centralized authentication, access and audit policy with access management.



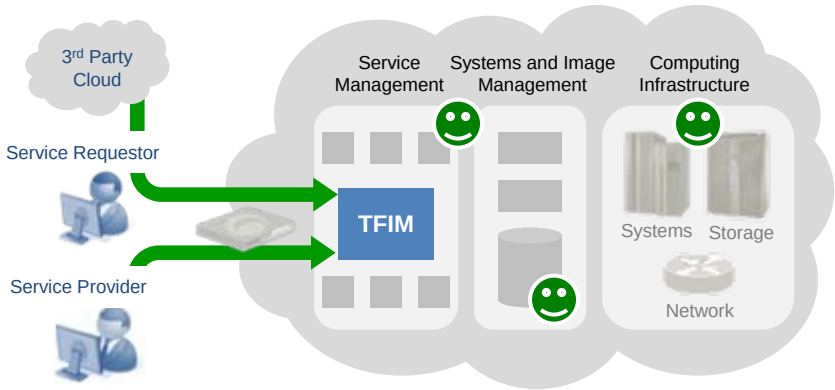
Tivoli Federated Identity Manager (TFIM)

Cloud Identity Federation

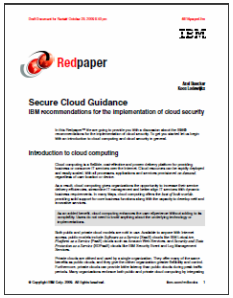
Single access method for users into cloud and traditional applications

Summary: TFIM enables trust between SOA-based initiatives by connecting users to services across business domains and helps enterprises strengthen and automate user access rights.

Cloud Use Case: In massively parallel, cloud-computing infrastructures, which involve enormous pools of external users constantly logging in to leverage IT services, TFIM's many authentication management features deliver significant business value.



IBM Security Framework



IBM Cloud Security Guidance Document

Data and Information

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

Ensure confidential data protection

- Protect PII and Intellectual Property
- Implement a secure key management program
- 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.

Data and Information

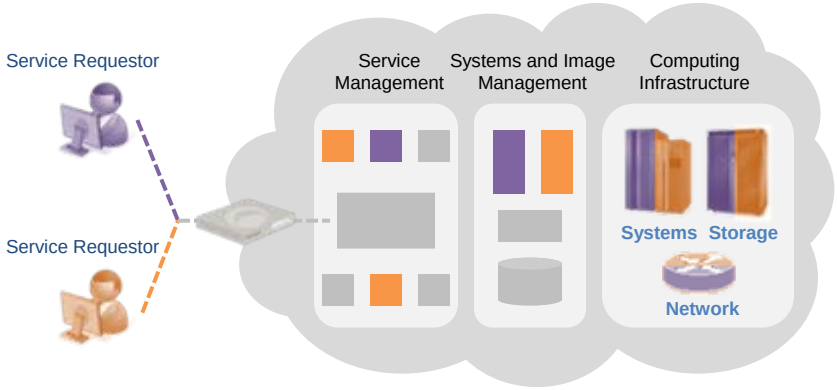
Data Segregation

Managing shared data resources within a multi-tenant environment

IBM Systems, Storage, and Network Segmentation

Summary: Designed to be shared by thousands of users, the IBM server has security built into nearly every level of the computer - from the processor to the OS to the application level. IBM is also an industry leader in providing storage solutions that maintain isolation within a multi-site enterprise infrastructure.

Cloud Use Case: Application isolation, OS containers, encrypted storage, VLANs and other isolation technologies can help provide a secure multi-tenant cloud infrastructure.



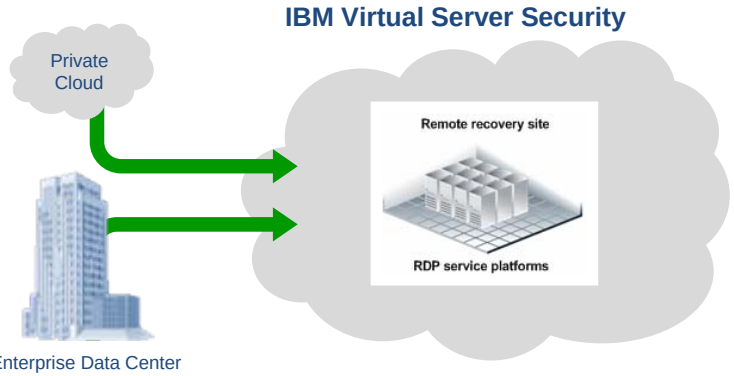
Hypervisor isolation

Separation of multi tenant systems

IBM Virtual Server Security

Summary: Firewall and intrusion prevention, integration at the hypervisor level, VMSafe. Virtual network segment protection, virtual netwrok access control

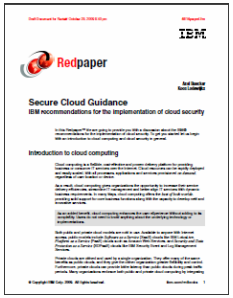
Cloud Use Case: Multiple operating systems and applications per physical server need to be monitored from a security perspective based on the fact that many companies data may be residing on the same physical server.



IBM Security Framework

Application and Process

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



IBM Cloud Security Guidance Document

Establish application and environment provisioning

- Implement a program for application and image provisioning.
- Ensure provisioning management is strictly controlled
- Protect machine images from corruption and abuse
- Ensure all changes to virtual images and applications are logged.
- Ensure provisioned images apply appropriate access rights
- Ensure destruction of outdated images

Application and Process

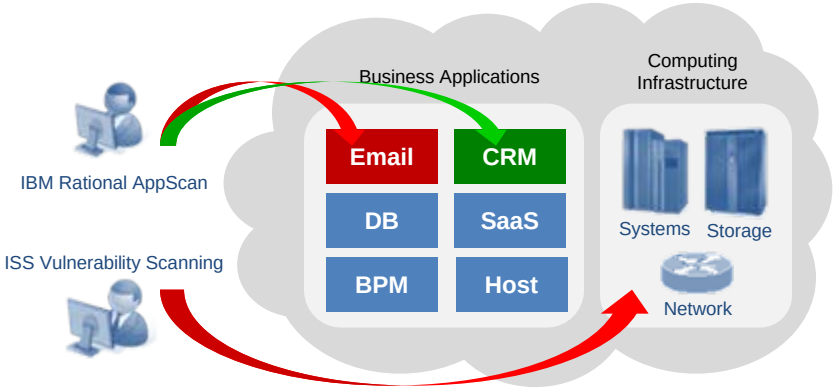
Compliance and Auditing

Vulnerability and compliance checking of cloud applications

IBM Rational AppScan & IBM Vulnerability Assessment Services

Summary: IBM Rational AppScan scans and tests for common Web application vulnerabilities including SQL-Injection, Cross-Site Scripting and Buffer Overflow. IBM ISS Professional Security Services performs automated scans to identify operating systems, apps, and their respective vulnerabilities.

Cloud Use Case: External or internal testing of cloud applications and their hosted infrastructure. Delivered as components for integration into the cloud or as a hosted service via-the-cloud.



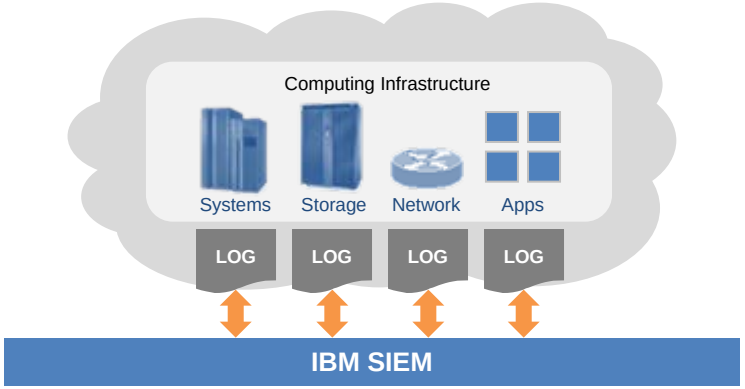
Investigative Support

Ability to inspect and audit a cloud provider's logs and records

IBM Security Information and Event Management

Summary: The IBM Security, Information and Event and Log Management solution enables corporations to compile event and log files from network devices, applications, databases and operating systems, as well as security technologies, into one seamless platform – administered from an easy-to-use Web portal.

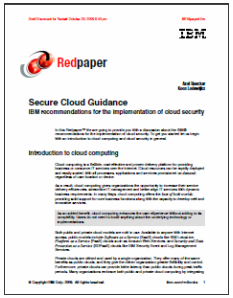
Cloud Use Case: Improves the speed of conducting security investigation and archives forensically-sound data, admissible as evidence in a court of law, for a period up to seven years.



IBM Security Framework

Network, Server and End Point

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



IBM Cloud Security Guidance Document

Maintain environment testing and vulnerability/intrusion management

- Implement vulnerability scanning, anti-virus, intrusion detection and prevention on all appropriate images
- Ensure isolation exists between tenant domains
- Trusted virtual domains: policy-based security zones
- A secure application testing program should be implemented.
- Develop all Web based applications using secure coding guidelines.
- Ensure external facing Web applications are black box tested

Network, Server, and Endpoint

Enterprise Security

Security for existing IT infrastructure as it extends to the cloud

IBM Enterprise Security Solutions

Summary: IBM security products and services driven by X-Force research, Tivoli Security Software to reduce cost and risk, and IBM Systems work together to create a highly secure computing environment that minimizes the potential risk posed by security threats.

Cloud Use Case: Our end-to-end solutions allow customers to build a strong security posture - positioning them to reap the rewards of emerging trends such as cloud computing.

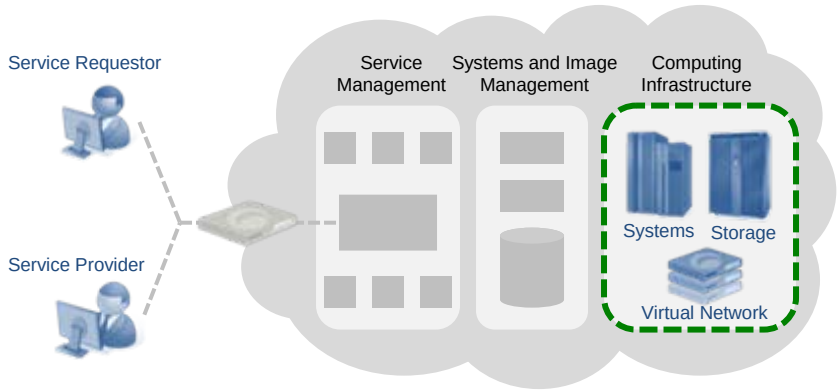
Virtualization Security

Security for pools of high performance virtualized resources

IBM Systems and IBM Virtualization Security

Summary: IBM offers the industry's broadest set of virtualization capabilities. Relying on over 40 years of heritage and attention to security, IBM virtualization platforms are built with security as a requirement, not an afterthought. Solutions from IBM ISS, such as Proventia Server and virtual appliances, strengthen defenses by eliminating additional threats.

Cloud Use Case: Security of the virtualization stack - enabling flexible, rapid provisioning across heterogeneous servers and hypervisors.

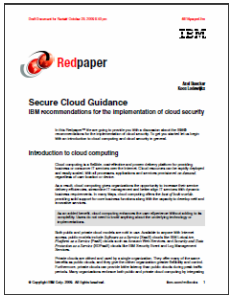


27

IBM Security Framework

Physical Security

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



IBM Cloud Security Guidance Document

Implement a physical environment security plan

- Ensure the facility has appropriate controls to monitor access.
- Prevent unauthorized entrance to critical areas within facilities e.g. servers, routers, storage, power supplies
- Biometric access of employees
- Ensure that all employees with direct access to systems have full background checks.
- Provide adequate protection against natural disasters.

Physical Infrastructure

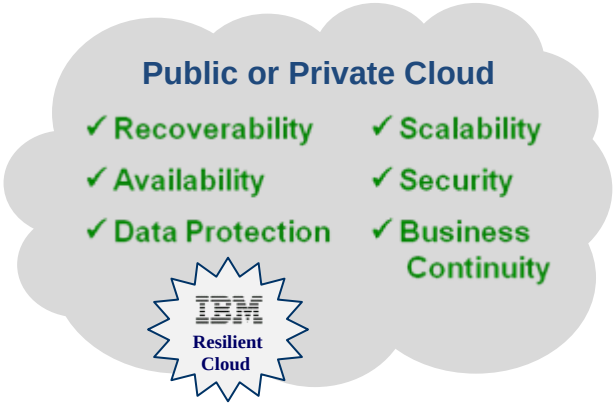
Disaster Recovery

Restoration and availability of cloud computing resources

BCRS Resilient Cloud Validation Program

Summary: IBM Business Continuity and Resiliency Services (BCRS) plans to offer a validation program in early 2009 for cloud service providers to ensure the resiliency of their business.

Cloud Use Case: By using proven BCRS resiliency consulting methodology, combined with traditional shared and dedicated asset business and resiliency managed services, IBM is positioning BCRS as the premier resiliency provider to Cloud service providers.



Data Location

Ability to process data in specific jurisdictions according to local requirements

High Performance On Demand Solutions (HiPODS) + IBM ISS Security Operations Centers

Summary: HiPODS is a group of specialists within IBM's Software Strategy group, with seven cloud computing locations around the world. IBM also has eight Security Operations Centers (SOCs) with a global reach to serve clients with international capabilities and a local presence.

Cloud Use Case: The HiPODS team can create a project team anywhere in the world in minutes and assign servers / storage for a project in less than an hour. IBM SOCs monitor more than 17,000 security devices on behalf of 3,700 customers.

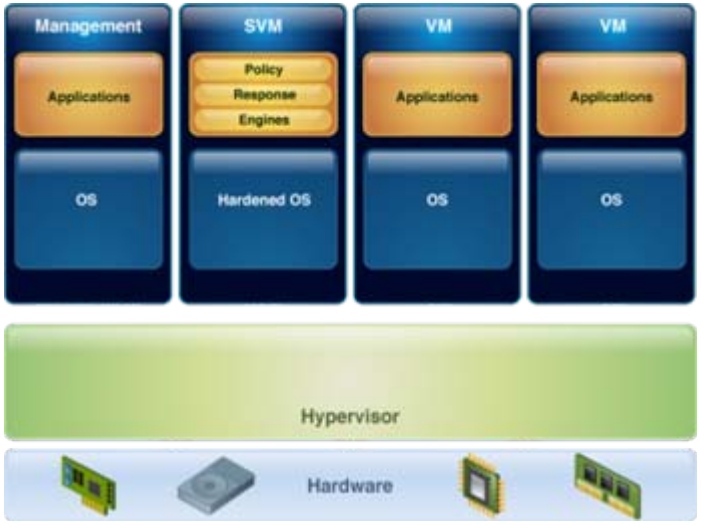
Security complexities raised by virtualization

- **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
  - Maintenance of virtual images
  - Backup/Disaster recovery
  - Geographic location of images, data
  - Demonstrating compliance using shared data

Before Virtualization

- 1:1 ratio of OSs and applications per server

After Virtualization

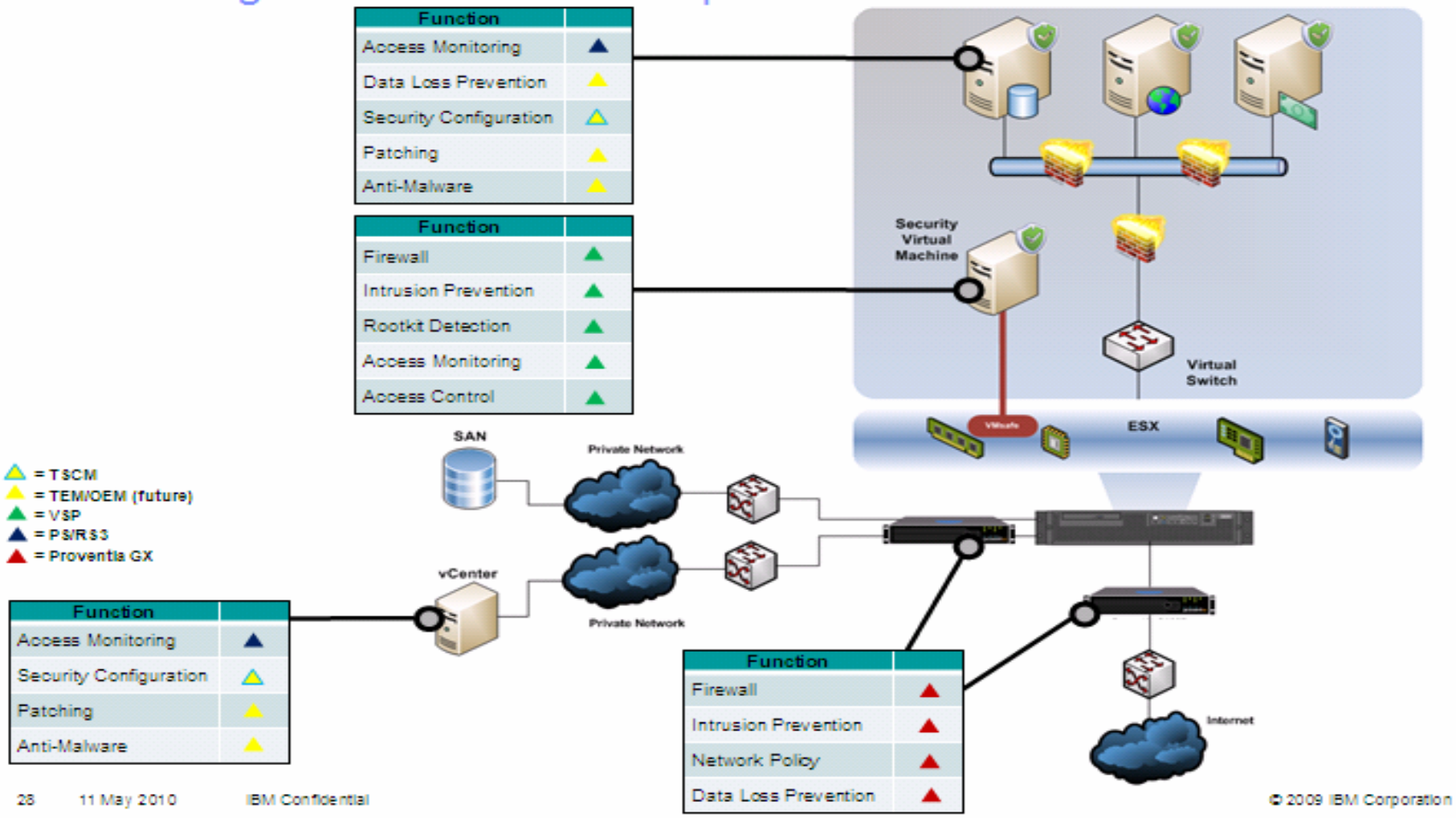


- 1:Many ratio of OSs and applications per server
- Additional layer to manage and secure

Cloud Delivered Services & Cloud Platform: Securing Virtual Machines

IBM

Threat Mitigation - Defense in Depth



Summary

- “Cloud” is a new consumption and delivery model inspired by consumer Internet services.
- Security Remains the Top Concern for Cloud Adoption
- One sized security doesn’t fit all
- Take a structured approach to securing your cloud environment
- Documented guidance is available for download to assist you in securing your cloud environment
- IBM has a view from End to End when it addresses your security needs

Tool Talk Webcast:
Anatomy of the Advanced Persistent Threat

Wednesday, May 19 at 1:00 PM EDT (1700 UTC/GMT)

https://www.sans.org/webcasts/anatomy-advanced-persistent-threat-93388

IBM X-Force manager Tom Cross will lead a 45-minute session dissecting a sample attack and outlining the defense strategies enterprises should take to protect themselves.

Protect your enterprise network by first understanding the threat - how it works, who it targets and what's at risk? Security experts from SANS and the IBM X-Force Research & Development team will dissect a sample attack representative of the Advanced Persistent Threat. This webcast will demystify the hype around today's top network concerns and provide the knowledge you need to plan your organization's defenses against the Advanced Persistent Threat.

Proventia GX Version 2 - Network Intrusion Prevention Appliances!!!

Proventia GX Hardware Refresh 2Q 2010
(Performance Enhanced)

- GX4004-V2
- GX5008-V2
- GX5108-V2
- GX5208-V2

- Multi-Core CPU's
- Next Generation hardware design
- Content Analysis performance headroom Performance Optimization
- Significant price/performance improvement
- 64 Bit PAM

IBM provides Enterprise-grade Security for Cloud Computing

Who can do this better than IBM?

…Nobody

Thank you!

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