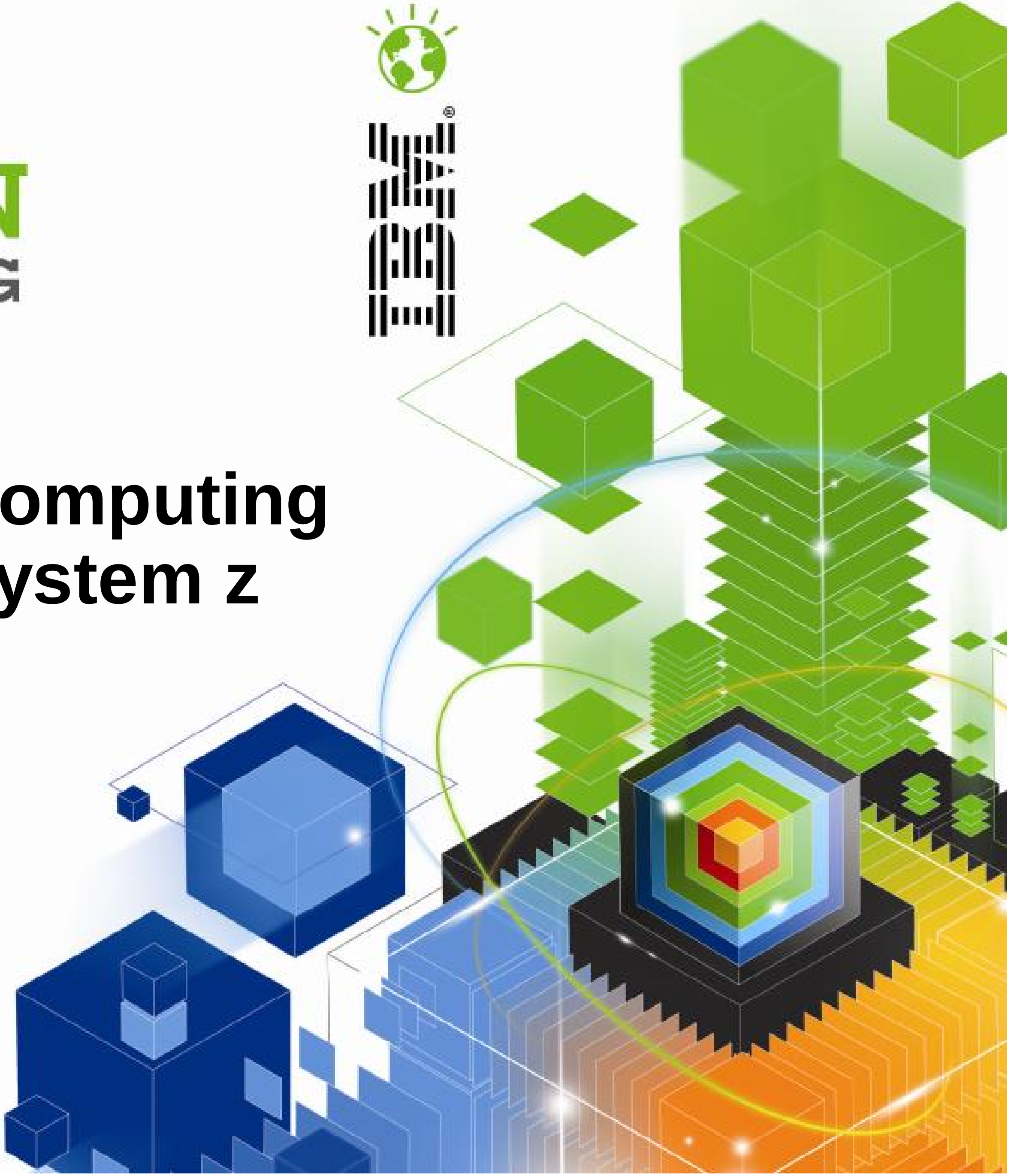
zEnterprise

A NEW DIMENSION IN COMPUTING

Secure Cloud Computing with Linux on System z

Siegfried Langer
Business Development Manager
z/VSE & Linux on System z



Discussion Topics

- Brief introduction to Cloud Computing
- Security: grand challenge for the adoption of Cloud Computing
- Security features of System z, z/VM, and Linux on System z
- Best practices

Cloud computing is about enabling the end user to help themselves

A user experience and a business model

- Standardized offerings
- Rapidly provisioned
- Flexibly priced
- Ease of access

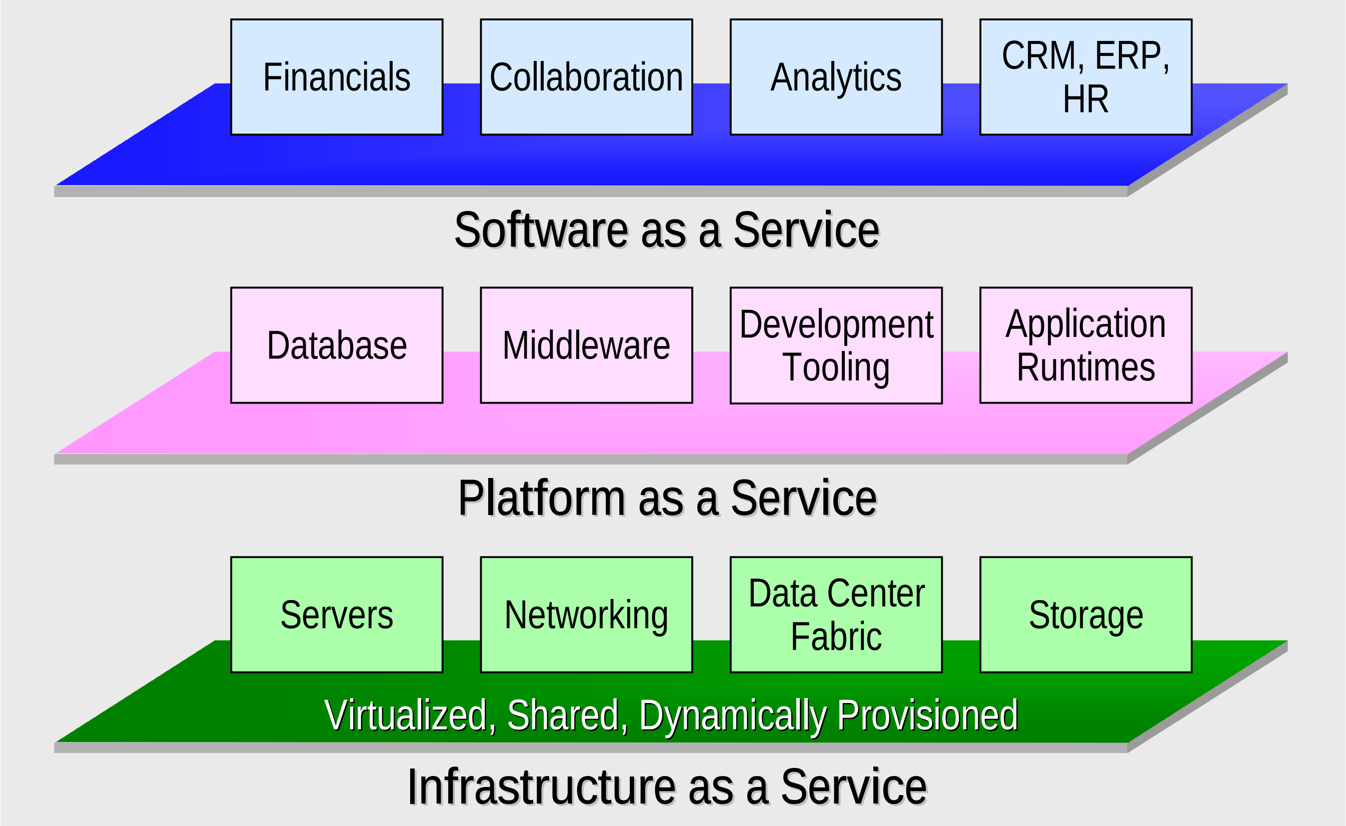
An infrastructure management and services delivery method

- Virtualized resources
- Managed as a single large resource
- Delivering services with elastic scaling

Similar to Banking ATMs and Retail Point of Sale, Cloud is Driven by:

- Self-Service
- Economies of Scale
- Technology Advancement

Cloud Service Models



EXAMPLES:

IBM Smart Analytics Cloud for System z

IBM WebSphere CloudBurst Appliance

IBM System z Solution Edition for Cloud Computing

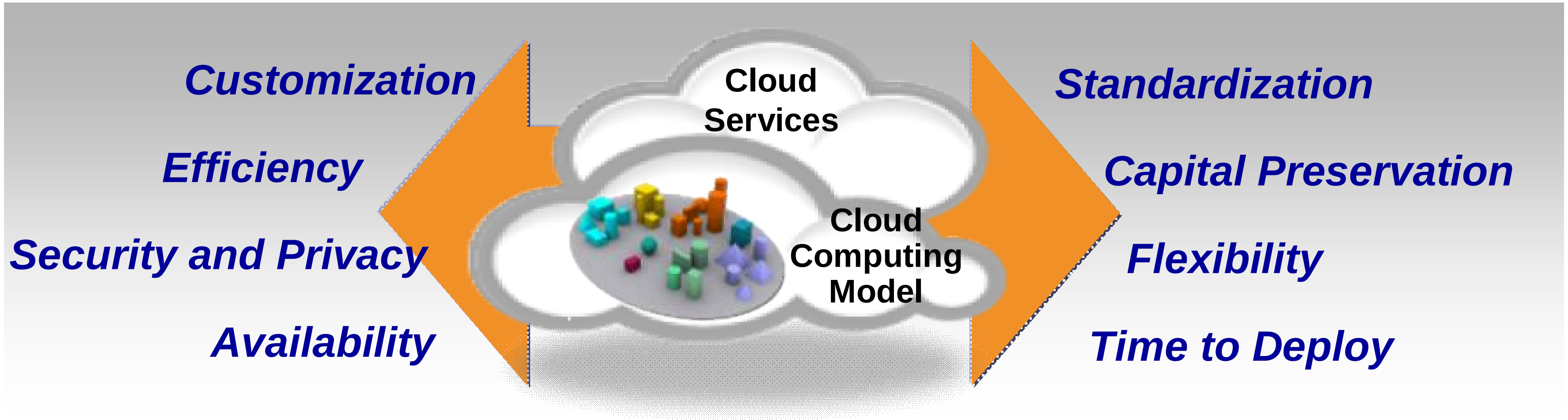
Cloud Computing can be implemented in many different ways

Private Cloud

- Client owned and managed
- Access limited to client and its partner network
- Drives efficiency, standardization and best practices while retaining greater customization and control

Public Cloud

- Service provider owned and managed
- Access by subscription
- Delivers select set of standardized business process, application and/or infrastructure services on a flexible price per use basis



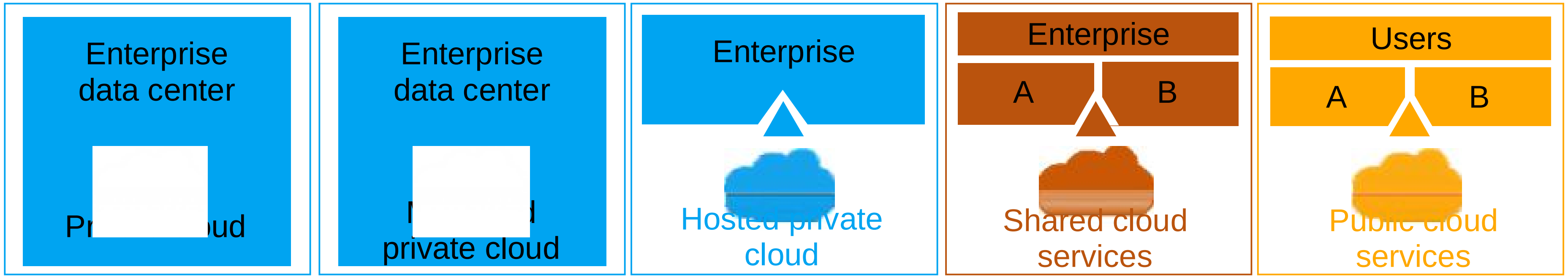
There is a spectrum of deployment options for cloud computing

Private

IT capabilities are provided "as a service," over an intranet, within the enterprise and behind the firewall

Public

IT activities / functions are provided "as a service," over the Internet

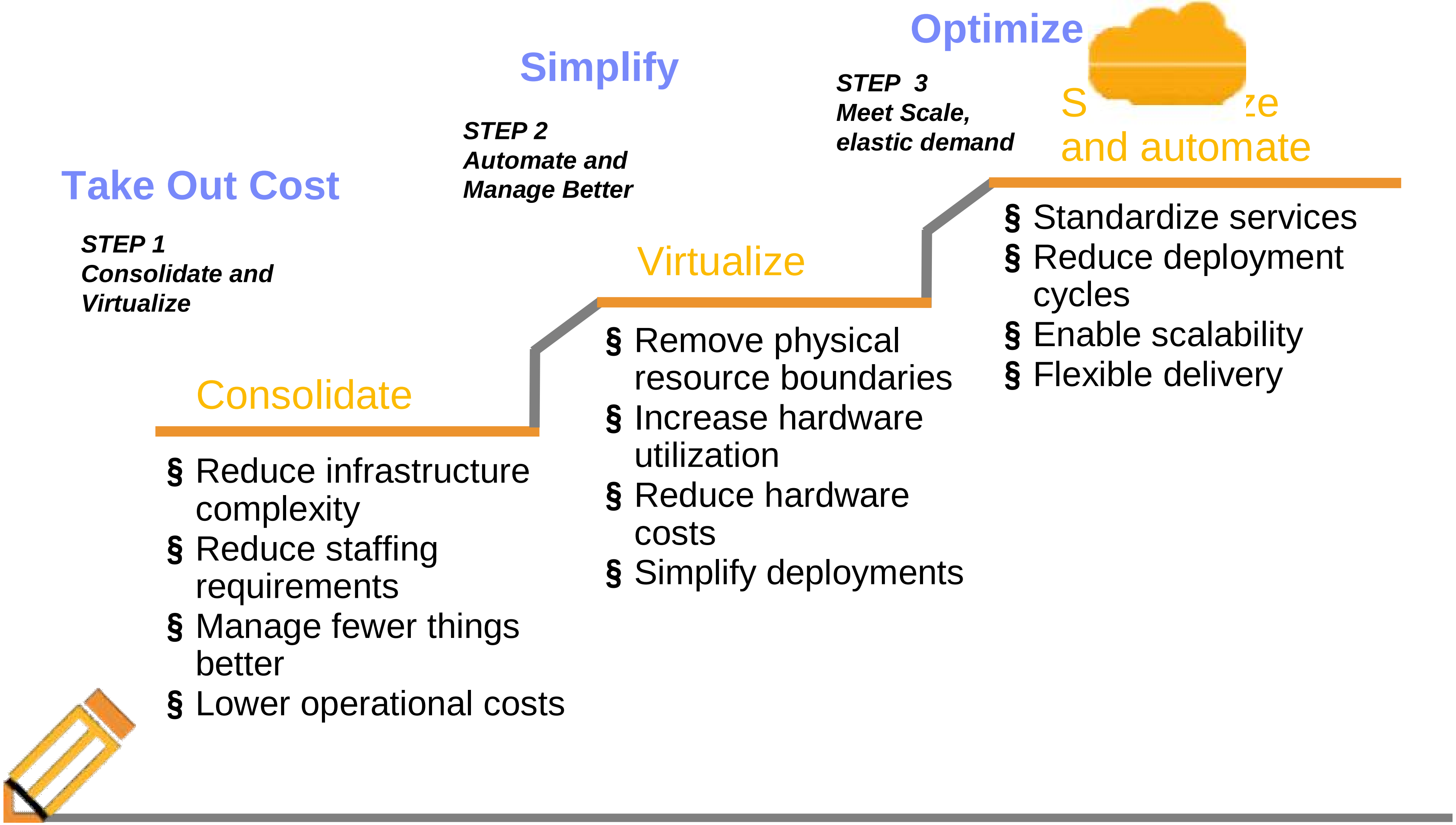


Third-party operated

Third-party hosted and operated

Hybrid **Internal and external service delivery methods are integrated**

Integrate a cloud computing deployment as part of the existing IT optimization strategy and roadmap



Take Out Cost

STEP 1
Consolidate and
Virtualize

Consolidate

- Reduce infrastructure complexity
- Reduce staffing requirements
- Manage fewer things better
- Lower operational costs

Simplify

STEP 2
Automate and
Manage Better

Virtualize

- Remove physical resource boundaries
- Increase hardware utilization
- Reduce hardware costs
- Simplify deployments

Optimize

STEP 3
Meet Scale,
elastic demand

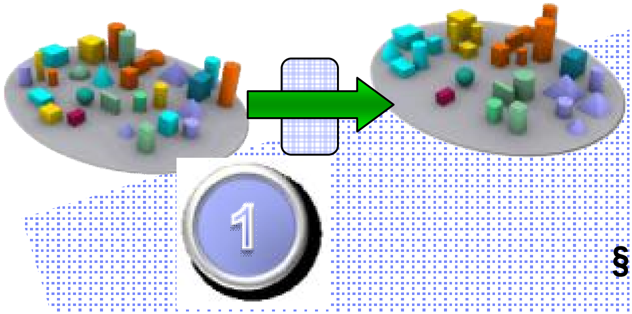
S ze
and automate

- Standardize services
- Reduce deployment cycles
- Enable scalability
- Flexible delivery

A Step-by-Step Approach for Growing Cloud on zEnterprise

Take Out Cost

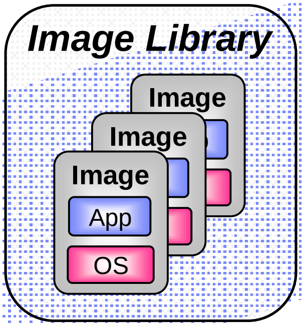
STEP 1
Consolidate and Virtualize



- Exploit the extreme virtualization capabilities of System z and z/VM
- Use basic z/VM features and functions to manage virtual Linux servers

Simplify

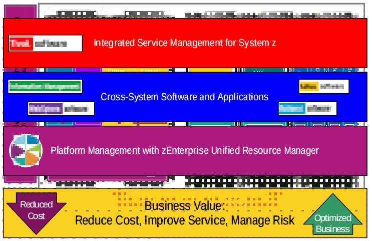
STEP 2
Automate and Manage Better



- Use advanced z/VM features and functions for automated operations and service delivery
- Introduce Systems Director for additional image management
- Add Tivoli technologies for greater levels of service management

Integrate and Optimize

STEP 3
Cross-architecture Workload Optimization


Integrated Service Management for System z
Cross-System Software and Applications
Platform Management with zEnterprise Unified Resource Manager
Reduced Cost
Business Value:
Reduce Cost, Improve Service, Manage Risk
Optimized Business

- zEnterprise is the industry's only multi-architecture cloud solution
- Use a cloud deployment model to host multi-tier solutions across System z, POWER and System x resources
- Use the Unified Resource Manager and Tivoli ISM for optimal workload placement

Cloud Offerings and Products

Enterprise Linux Server (z10, z196) Solution Edition for Enterprise Linux	IBM Systems Director and VMControl Solution Edition for Cloud Computing	zEnterprise System and zManager Tivoli Integrated Service Management

Discussion Topics

- Brief introduction to Cloud Computing
- **Security: grand challenge for the adoption of Cloud Computing**
- Security features of System z, z/VM, and Linux on System z
- Best practices

Security Remains 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

The Importance of Security

Loss of customer data at BNY Mellon much bigger than first thought

Bank confirms tape with info on 12 million customers of its shareholder service unit is unaccounted for

Sept 2, 2008

Massive insider breach at DuPont

A research chemist who worked for DuPont for 10 years before accepting a job with a competitor downloaded 22,000 sensitive documents

Feb 15, 2007

Societe Génerale loses $7.2 billion in trading fraud

Lack of privileged password management and insufficient IT security controls

Jan 24, 2008

The Goal of Information Security

§ **Ensure that the IT-related risk of *each party* is lowered to an *acceptable* level**

Categories of Tools:

- Risk Management Processes:
  - Understand your assets and their security objectives
  - Understand your risks (and monitor emerging risks!)
  - Mitigate a subset of the risks
  - Accept the residual subset of risks
- Security Controls to reduce given risks
  - Prevention (e.g., no-go-decisions, avoiding or blocking)
  - Detection (e.g. monitoring or audits)
  - Compensation (e.g., recovery or fail-over)

Real-life Example: Clouds cannot be more secure than their physical datacenters.

Why is Cloud Security Perceived as Such a Big Problem?

We Have Control

It's located at X.

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

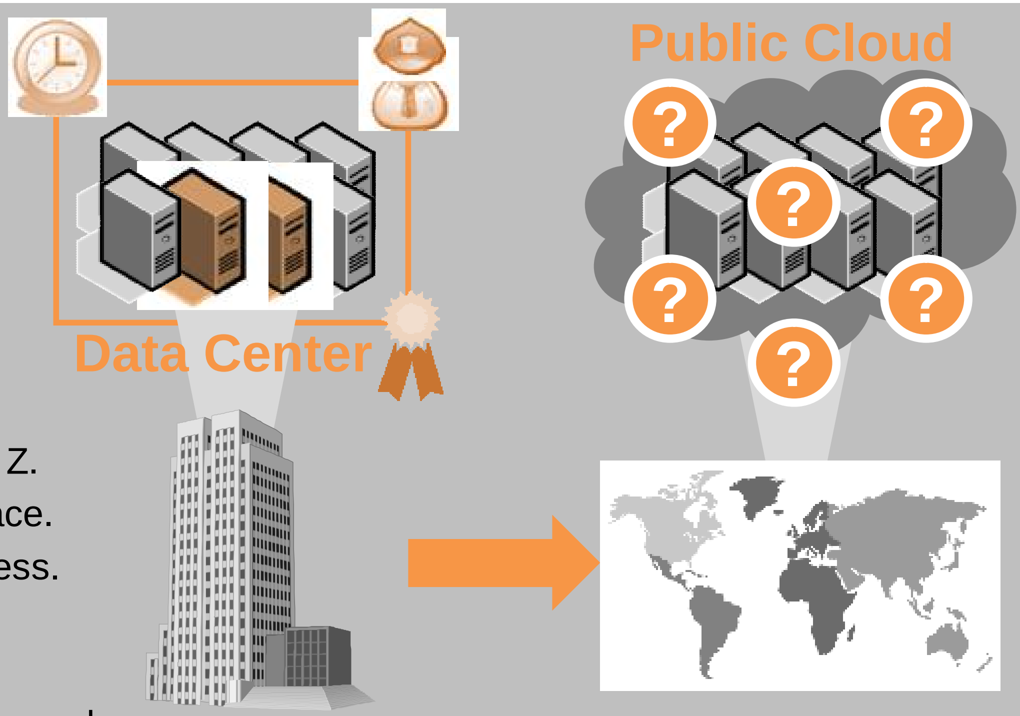
We have backups in place.

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?

- Loss of control, perceived or real
- Lack of experience
- No established standards
- Uncertainty on how to interpret regulations and practices

- Effects
  - Public clouds rarely used for mission critical workloads
  - Preference for application-as-a-service
  - Preference for private and hybrid cloud

Guiding the conversation

IBM Security Framework

IBM Security Framework
SECURITY GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE
PEOPLE AND IDENTITY
DATA AND INFORMATION
APPLICATION AND PROCESS
NETWORK, SERVER AND END POINT
PHYSICAL INFRASTRUCTURE
Common Policy, Event Handling and Reporting
Professional services
Managed services
Hardware and software

Describes the business landscape of security

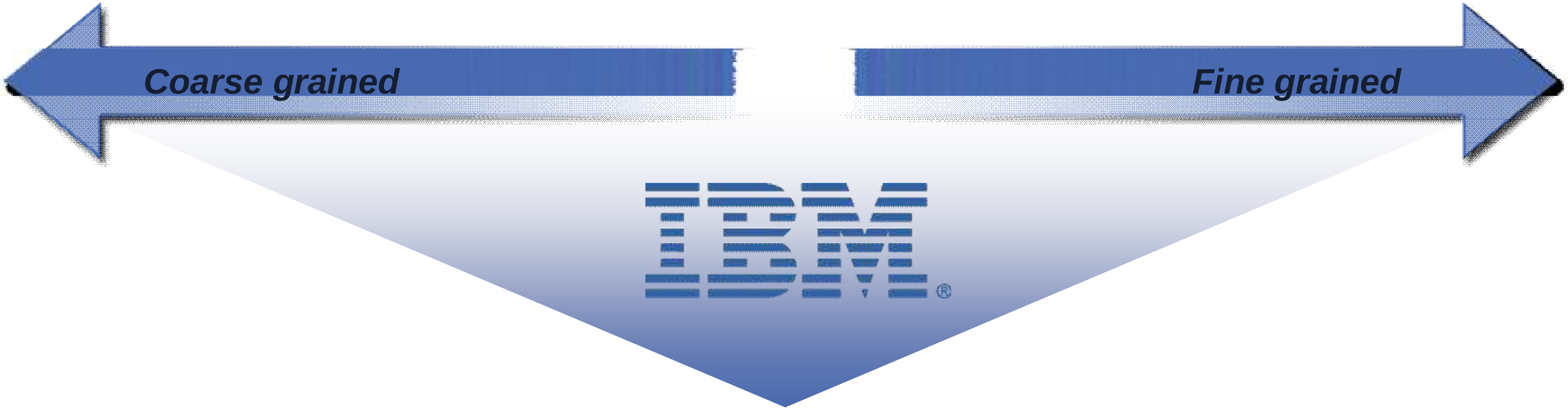
IBM Cloud Security Guidance

Redpaper
Secure Cloud Guidance
IBM recommendations for the implementation of cloud security
Introduction to cloud computing

Describes the technology landscape

IBM Capabilities & Offerings to Help

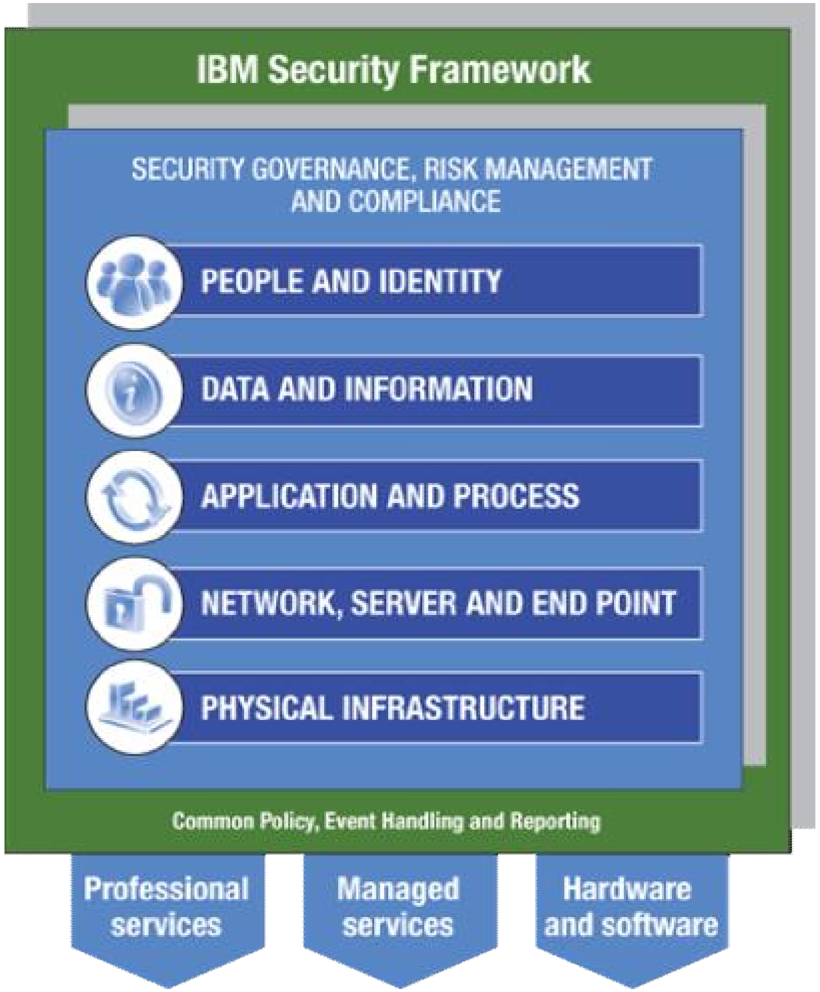
Catalogues of products, services and solutions



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*

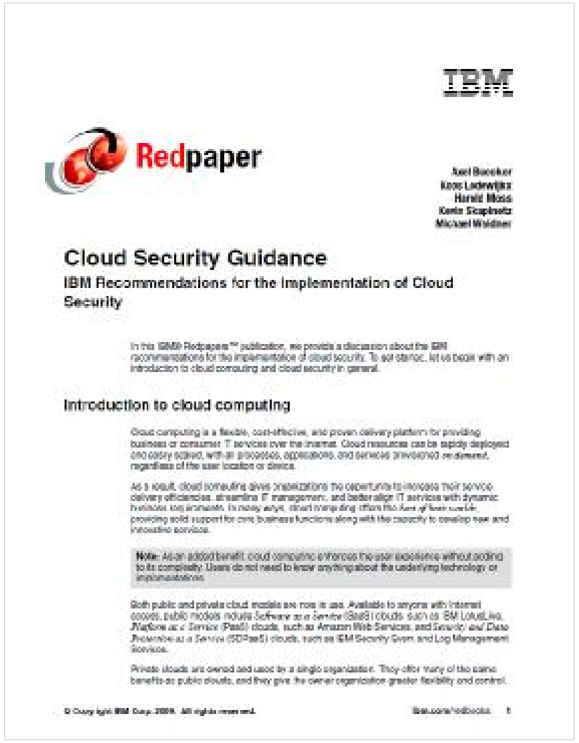


Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security;

IBM RedGuide REDP-4528-00, July 2009

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 Lodewijks
Harold Moss
Kevin Skapinetz
Michael Waidner

Cloud Security Guidance

IBM Recommendations for the Implementation of Cloud Security

In this IBM® Redpaper™ 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

IBM Security Blueprint Overview

Architectural Principles

IBM Security Framework: Business Security Reference Model

Governance, Risk, Compliance (GRC)

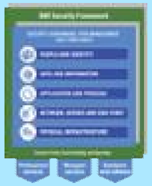
People & Identity

Data & Information

Application & Process

IT Infrastructure: Network, Server, End Point

Physical Infrastructure



Foundational Security Management

Software, System & Service Assurance

Identity, Access & Entitlement Mgmt

Data & Information Protection Mgmt

Threat & Vulnerability Management

IT Service Management

Command and Control Mgmt

Security Policy Management

Risk & Compliance Assessment

Physical Asset Management

Security Services and Infrastructure

Security Info and Event Infrastructure

Identity, Access & Entitlement Infrastructure

Security Policy Infrastructure

Cryptography, Key & Certificate Infrastructure

Network Security

Storage Security

Host and End-point Security

Application Security

Service Management and Process Automation

Physical Security

IT Security Services and Mechanisms

Security Service Level Objectives

Code & Images

Designs

Policies

Configuration Info and Registry

Identities & Attributes

Resources

Contexts

Data

Security Events & Logs

Knowledge

Security Controls – The Toolbox

Security Policy

- Enterprise, identity, access, retention, …
- Ideally derived and propagated top down
- Allow/deny + mandates/ obligations
- Often composite, mandatory and discr.
- Abstract, role based, class based

Security Development

- Practices
- Security testing
- Eg, OWASP

(www.owasp.org)

Prevention (Avoidance, Enforcement)	Detection (Monitoring, Audit)	Compensation (Recovery, Fail-over)

Cryptography

•Encryption
•Key management
•Channel security, VPN

•MAC, Hash
•Digital Signatures
•Message security

Redundancy

•Fault tolerance
•Backup & recovery
•Fail-over, graceful degradation

Access Control

•Reference monitor
•Authorization
•Data / proc tagging
•Hypervisor
•Memory protection
•Filesystem protection
•Virtual LAN

Intrusion / Extrusion Prevention

•Firewall
•Anti-virus, anti-malware
•Intrusion prevention
•Data leak prevention
•Virtual patching

Intrusion & Fraud Detection

•Signature-based
•Behavior-based
•Server, network based

Identity

•Authentication
•Identity Management

Trusted Computing

•Enforcement through (mutually) trusted hardware

Logging & Auditing

•Immutable logs
•Time stamping

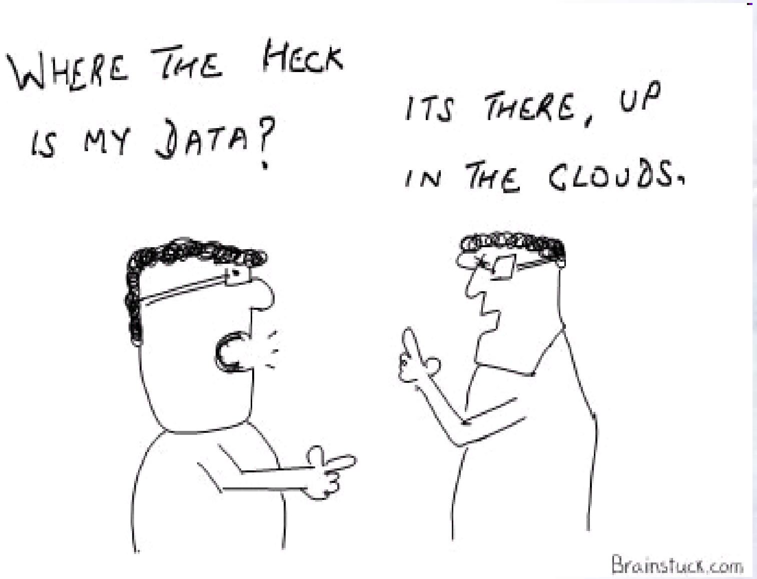
Asset Management
Change and Configuration Management
Physical and Organizational Security

Discussion Topics

- Brief introduction to Cloud Computing
- Security: grand challenge for the adoption of Cloud Computing
- Security features of System z, z/VM, and Linux on System z

  and

- Best practices



Reminder:
Information Security Process and Management System

- Information Security Risk Management requires

Policy and Process

Service Management and IT Governance

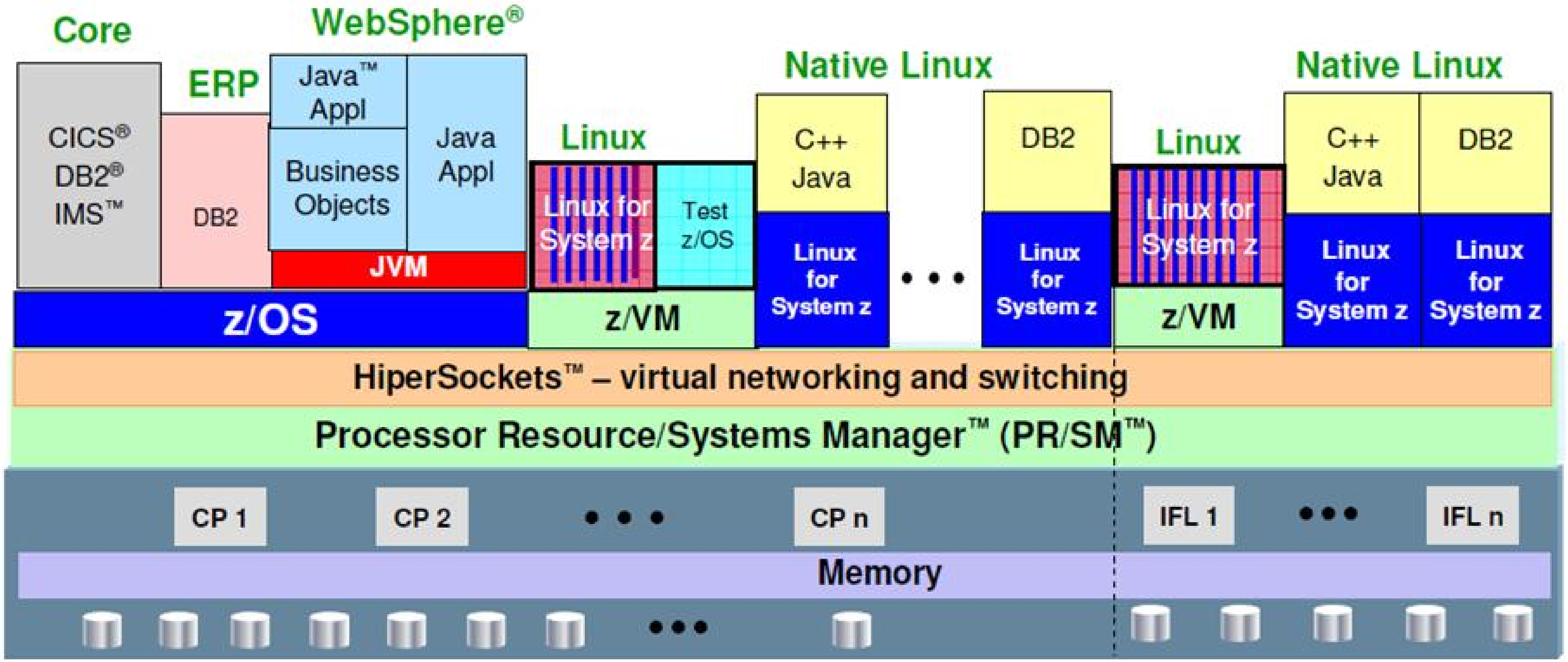
People and Organization

Education and Incentives

Measurement and Reporting

Our focus: and Security Technology

Models are Mixed in Real Life. Example: IBM System z



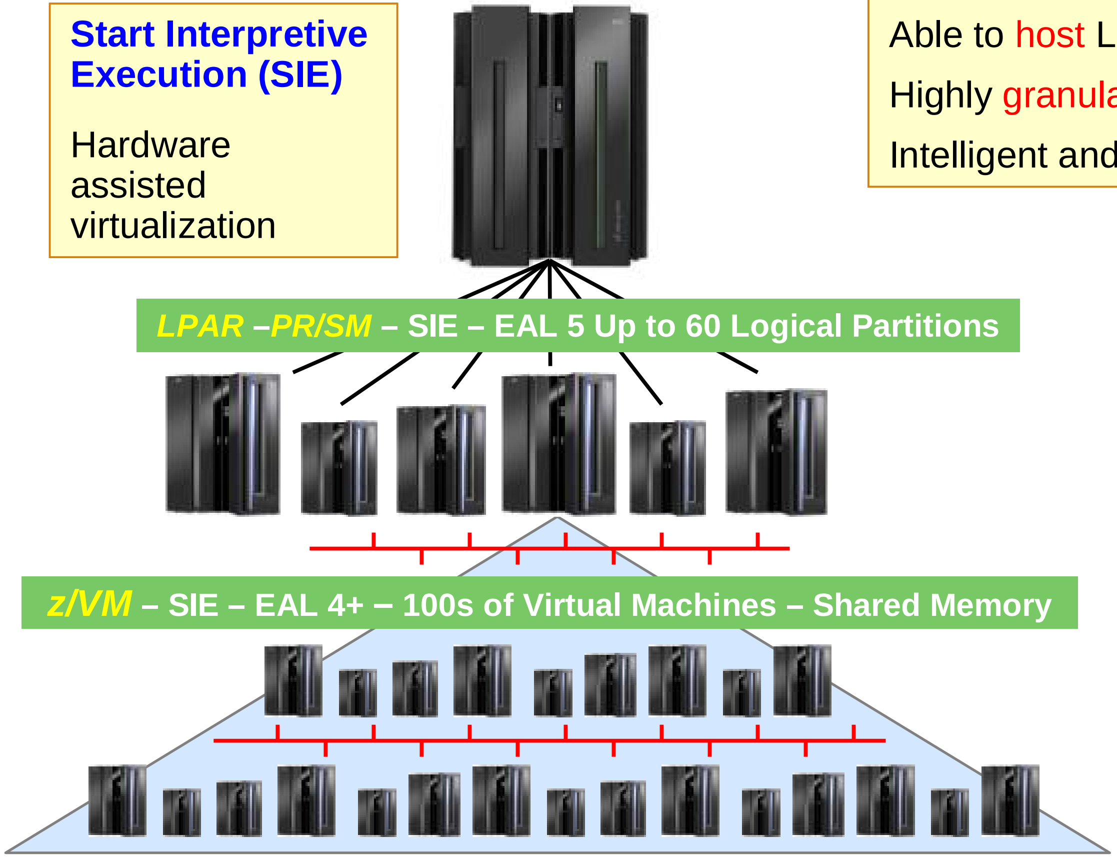
- Massive, robust consolidation platform; virtualization is built in, not added on
- Up to 60 logical partitions on PR/SM; 100's to 1000's of virtual servers on z/VM
- Virtual networking for memory-speed communication, as well as virtual layer 2 and layer 3 networks supported by z/VM
- Most sophisticated and complete hypervisor function available
- Intelligent and autonomic management of diverse workloads and system resources based on business policies and workload performance objectives

System z Multidimensional Virtualization Technology

Build-in and Shared Everything Architecture

Start Interpretive Execution (SIE)

Hardware assisted virtualization



LPAR –PR/SM – SIE – EAL 5 Up to 60 Logical Partitions

z/VM – SIE – EAL 4+ – 100s of Virtual Machines – Shared Memory

Maximum security and capacity isolation between virtual Linux servers

Most sophisticated and functionally complete hypervisors

Able to host Linux, OpenSolaris, z/OS, and z/VM-on-z/VM

Highly granular resource sharing (less than 1% utilization)

Intelligent and autonomic workload management

Shared executables and filesystems

Less administration and reduced memory

Internal high speed TCP/IP communication

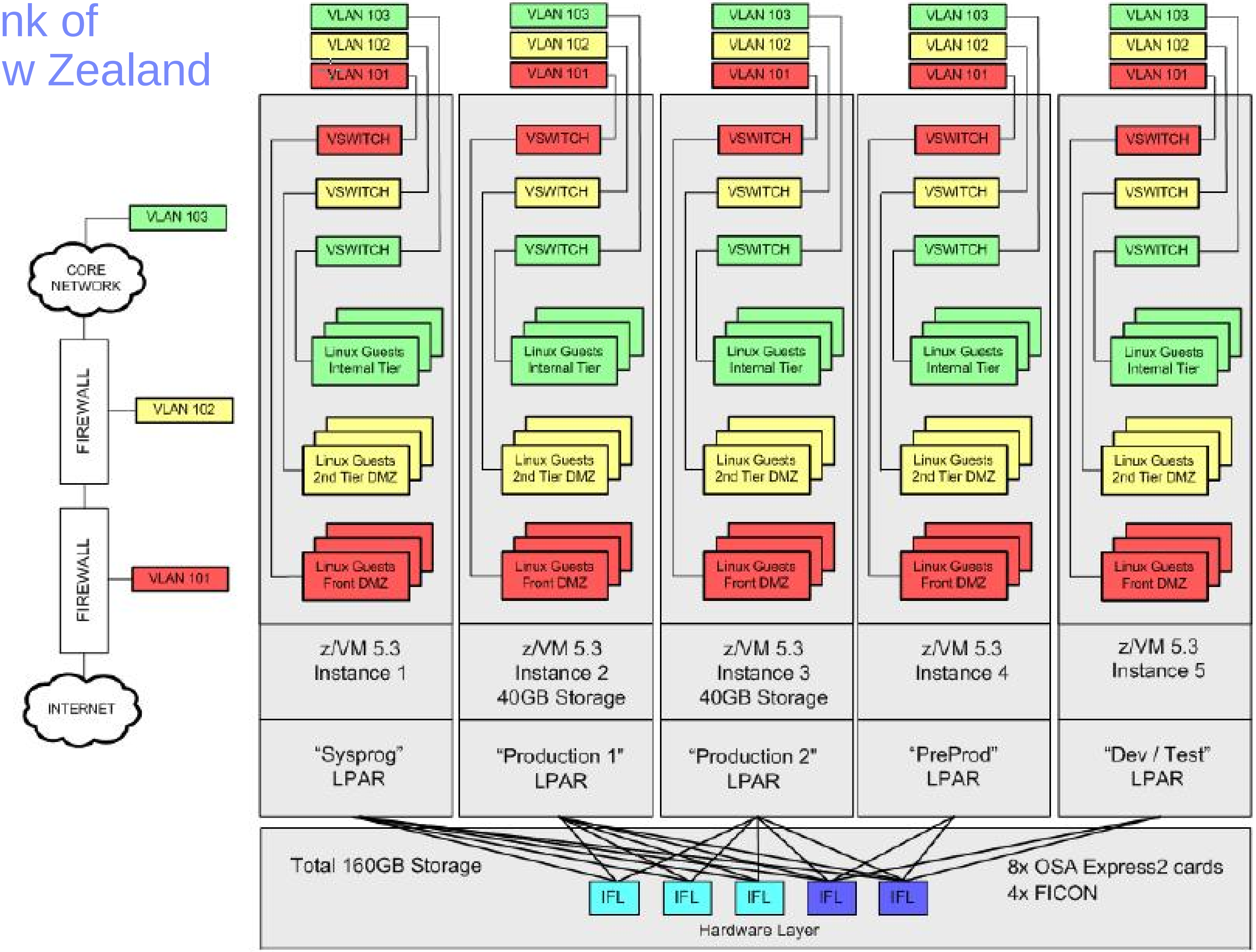
Hipersocket, VLAN, Virtual Switches, Virtual Routers, Virtual Firewalls

HW (LPAR) and SW (z/VM) hypervisors

Linux virtual servers runs on bare metal but under control of hypervisor.

I/O is transparent to hypervisor

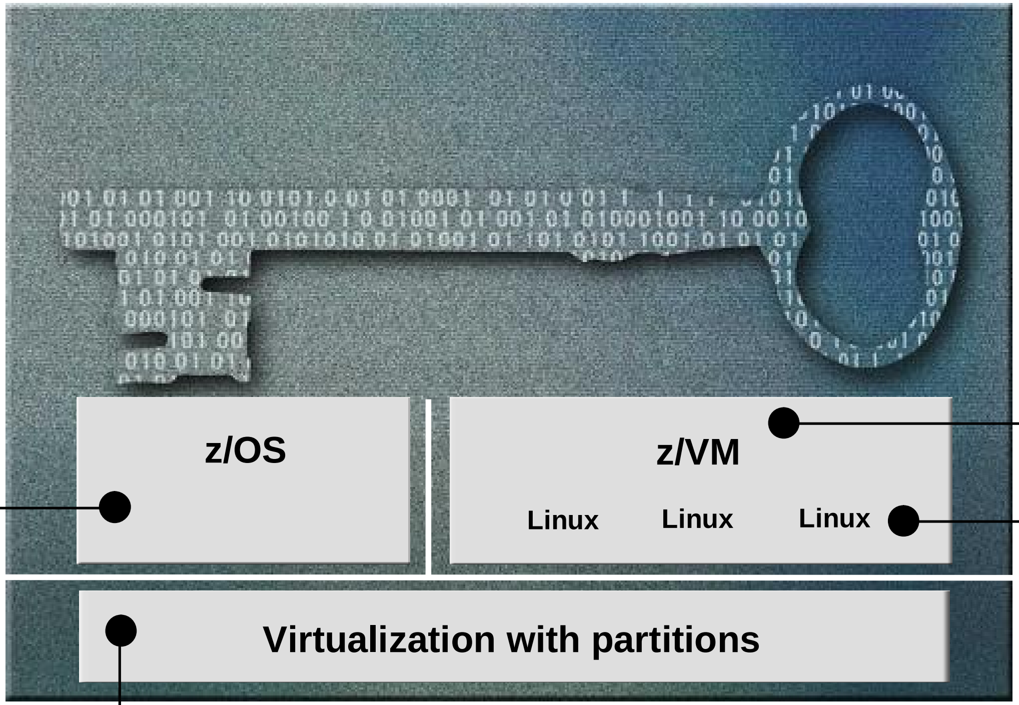
Bank of New Zealand



Certifications on System z

Security Server: RACF, LDAP, Firewall - Encryption - Public Key Infrastructures - Certificate Authority

The Common Criteria program developed by NIST and NSA establishes an organizational and technical framework to evaluate the trustworthiness of IT Products and protection profiles



z/OS

- **Common Criteria** EAL4+ with CAPP and LSPP
  - z/OS 1.9 + RACF
- **IdenTrust™** certification for z/OS PKI Services

System z EC and other System z servers

- **Common Criteria** EAL5 with specific Target of Evaluation
  - **Logical partitions**
- FIPS 140-2 level 4
  - Crypto Express as coprocessor

z/VM

- **Common Criteria** EAL4+ with CAPP and LSPP
  - **z/VM 5.3 + RACF**

Linux on System z

- **Common Criteria** EAL4+ with CAPP and LSPP
  - **SUSE LES9 certified**
- **Common Criteria** EAL3+ with CAPP and LSPP
  - **Red Hat EL4 certified at EAL4+**
  - **Red Hat EL5 EAL4+ in progress**

See: www.**ibm.com**/security/standards/st_evaluations.shtml

Security checklist for your virtual environment

At least take care of the following checklist:

- Protect your physical IT infrastructure
- Secure the logical access to z/VM
- Protect your data
- Protect your virtual network
- Secure the logical access to the Linux servers
- Protect your environment from yourself by keeping consistent and auditable system logs

Recommendations for securing the virtual environment (1)

- Use External Security Management (ESM), such as RACF
  - Securing the logical access to z/VM
  - Securing the data
  - Securing the network
  - Audit trail
- Choose the z/VM privilege classes
  - a Linux guest should only have access to its own virtual machines and resources
  - a Linux guest should not have additional privileges to define system-wide parameters of the z/VM system nor other virtual guests
- Implement mandatory access control (MAC)
- Centralized user repository, such as z/VM LDAP server or z/OS LDAP server

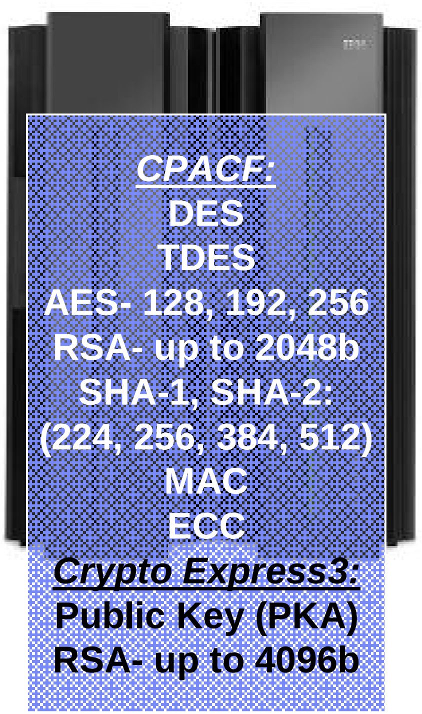
Recommendations for securing the virtual environment (2)

- All network access to z/VM (e.g. Telnet communication) should go through a secured channel, such as SSL
- Reduce intrusion points with shared disks
  - Golden rule on information management: information should only exist in one location
  - Ability to connect devices among guests within the same system (minimizing intrusion points)
- Protect the data with encrypted file systems
- Virtual switch using VLAN tagging and port isolation
  - Allows the data networks to be separated from management networks
- Separation of duties

System z cryptographic hardware

System z has two flavours for accelerating cryptographic operations:

- CP assists for symmetric algorithms (CPACF)
  - Hardware crypto accelerator is a standard feature on System z!
- Crypto cards (Crypto Express3) for asymmetric algorithms
  - Provide temper proof key storage and security module
  - Coprocessor and accelerator functionality



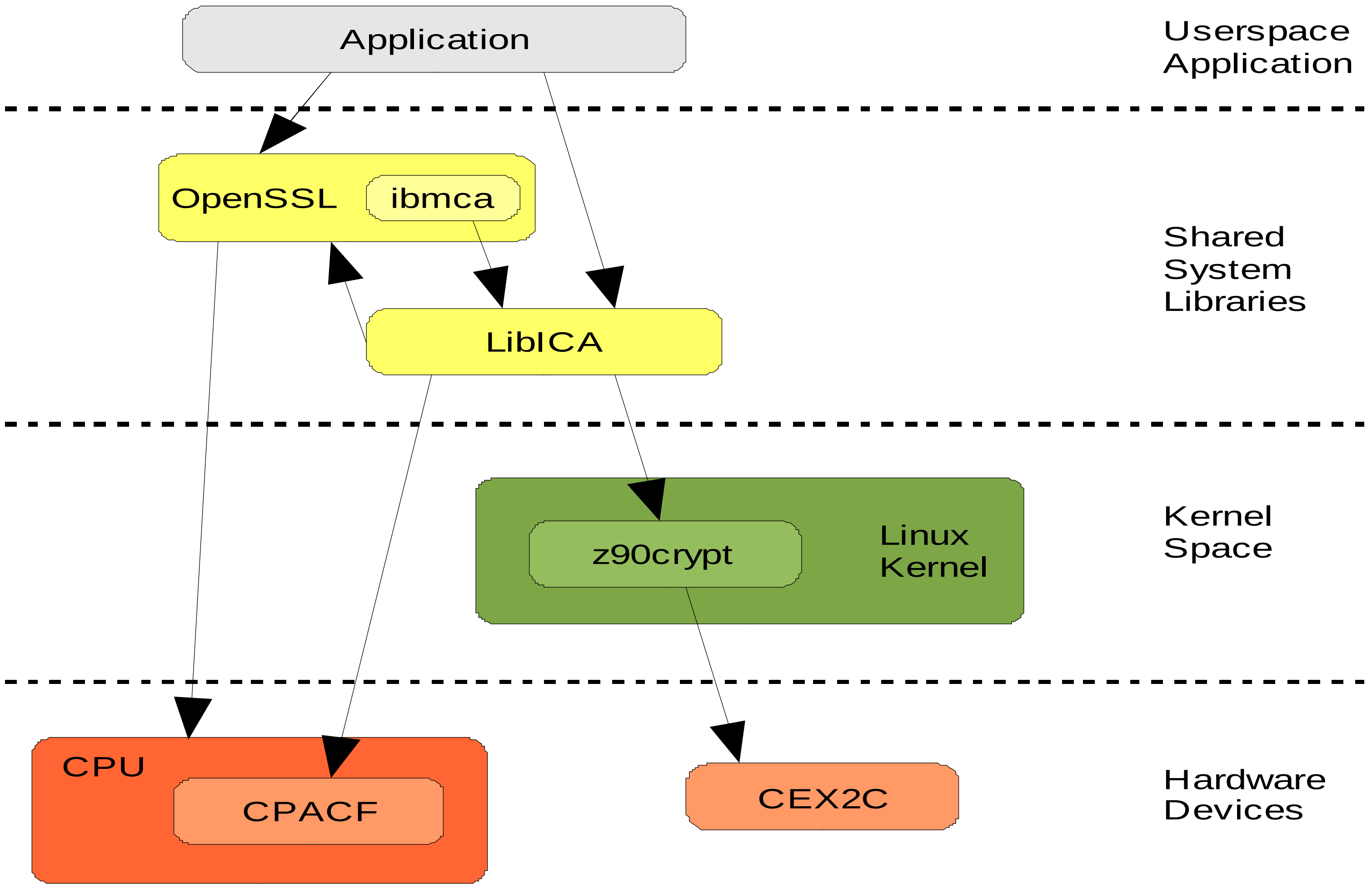
CPACF:
DES
TDES
AES- 128, 192, 256
RSA- up to 2048b
SHA-1, SHA-2:
(224, 256, 384, 512)
MAC
ECC

Crypto Express3:
Public Key (PKA)
RSA- up to 4096b

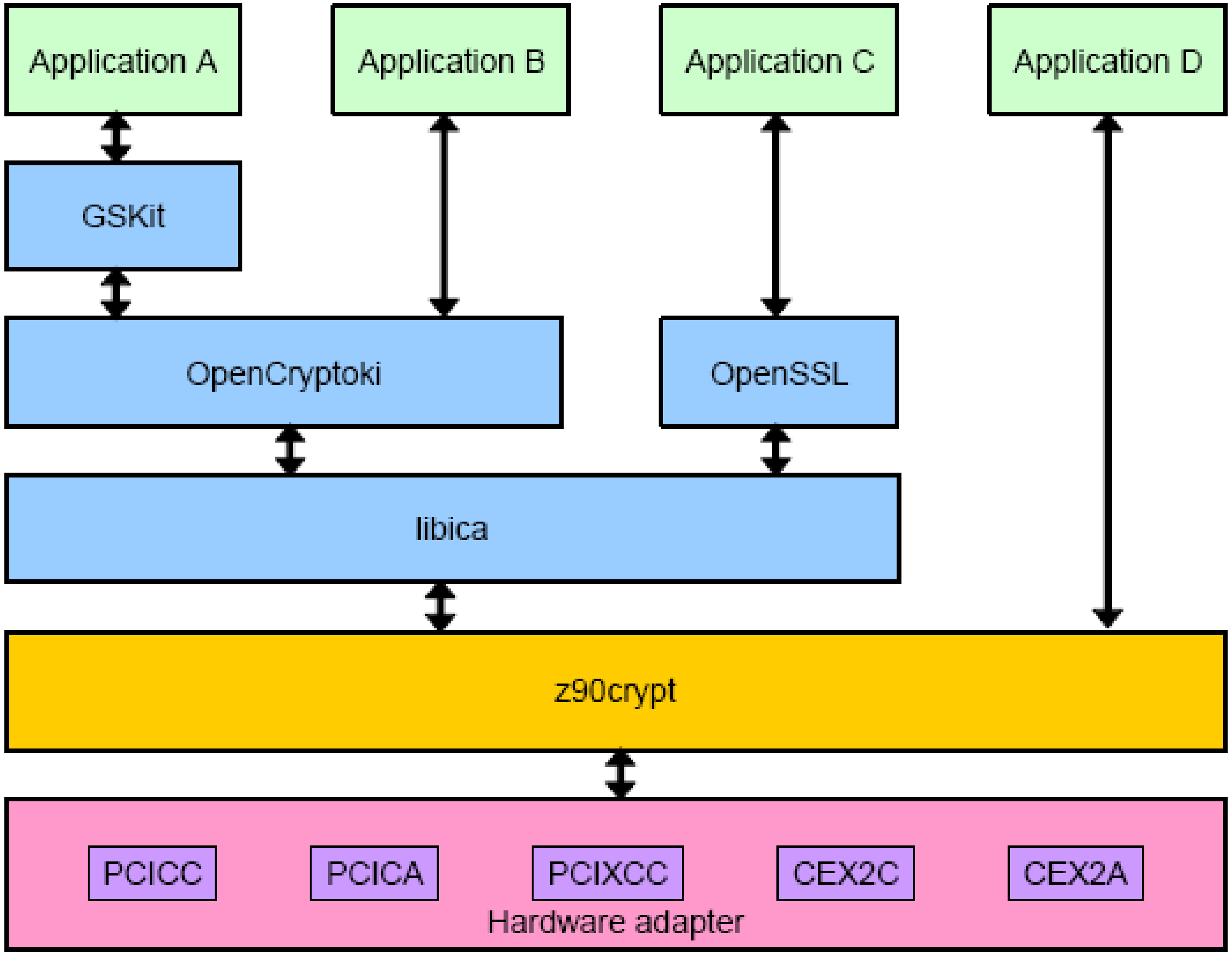
Purpose:

- Move cryptographic workload away from central processor
- Accelerate encryption / decryption
- Achieve higher security level
- Tight integration – no external connections (interception points)

Linux on System z Cryptography Support Overview

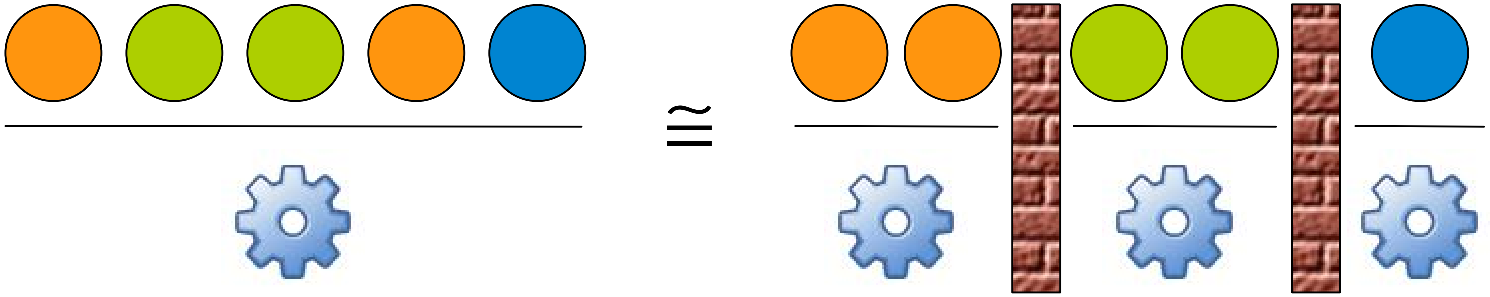


Cryptographic Libraries



Isolation and Integrity Management: Multi-tenancy

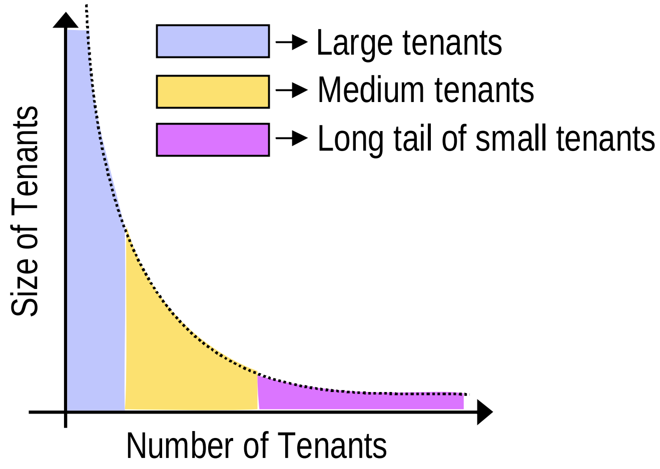
- Users from ***different* trust domains** are drawing on a ***shared* pool** of resources
  - Network, storage and server virtualization
  - Shared file system, database, middleware, application, desktop, business service, ...
  - Stack architectures offer choices for implementing multi-tenancy (lower or higher in the stack)
  - Isolation is the key security requirement
- Basic mechanism is *coloring* (aka *tagging, labeling*) and enforcement of isolation between *domains* (aka *zones*) of different colors

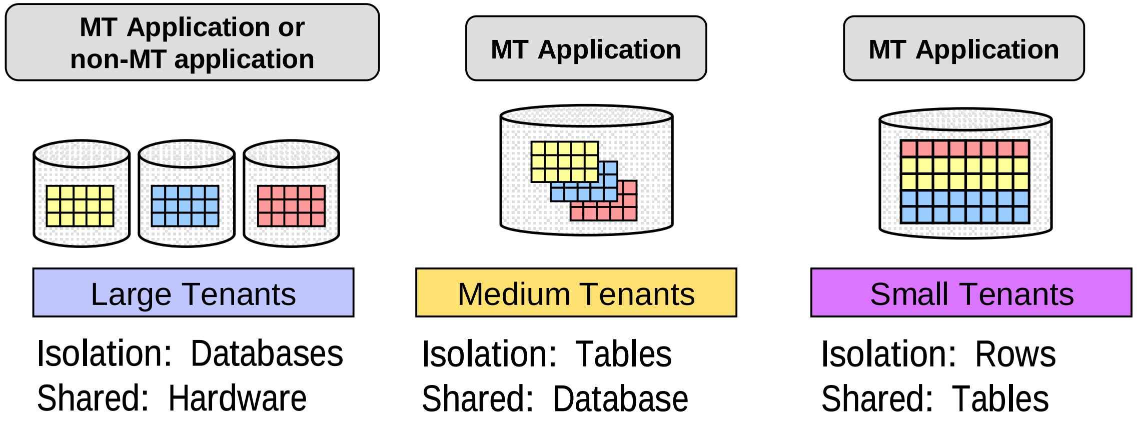


  - Enforcement through
    - Reference Monitor: provisioning, runtime, de-provisioning / cleanup
    - Hardware enforced zoning
    - Cryptography (encryption, key management)

Database-as-a-Service and Multi-tenancy with DB2

- **Multi-tenancy: multiple companies or users using the same software with a level of isolation**
  - Tenants are companies or users that would have historically installed and used a single instance of software solely for their own use
  - Multi-tenancy allows companies/users to use the same software with a level of isolation
- **Multi-tenancy can further reduce hardware and maintenance costs of DBaaS**
- **Analogous to users running various applications on the same operating system**
  - The point is to share management and hardware costs among a number of tenants
  - Tenants, like the distinct users on an operating system require a level isolation

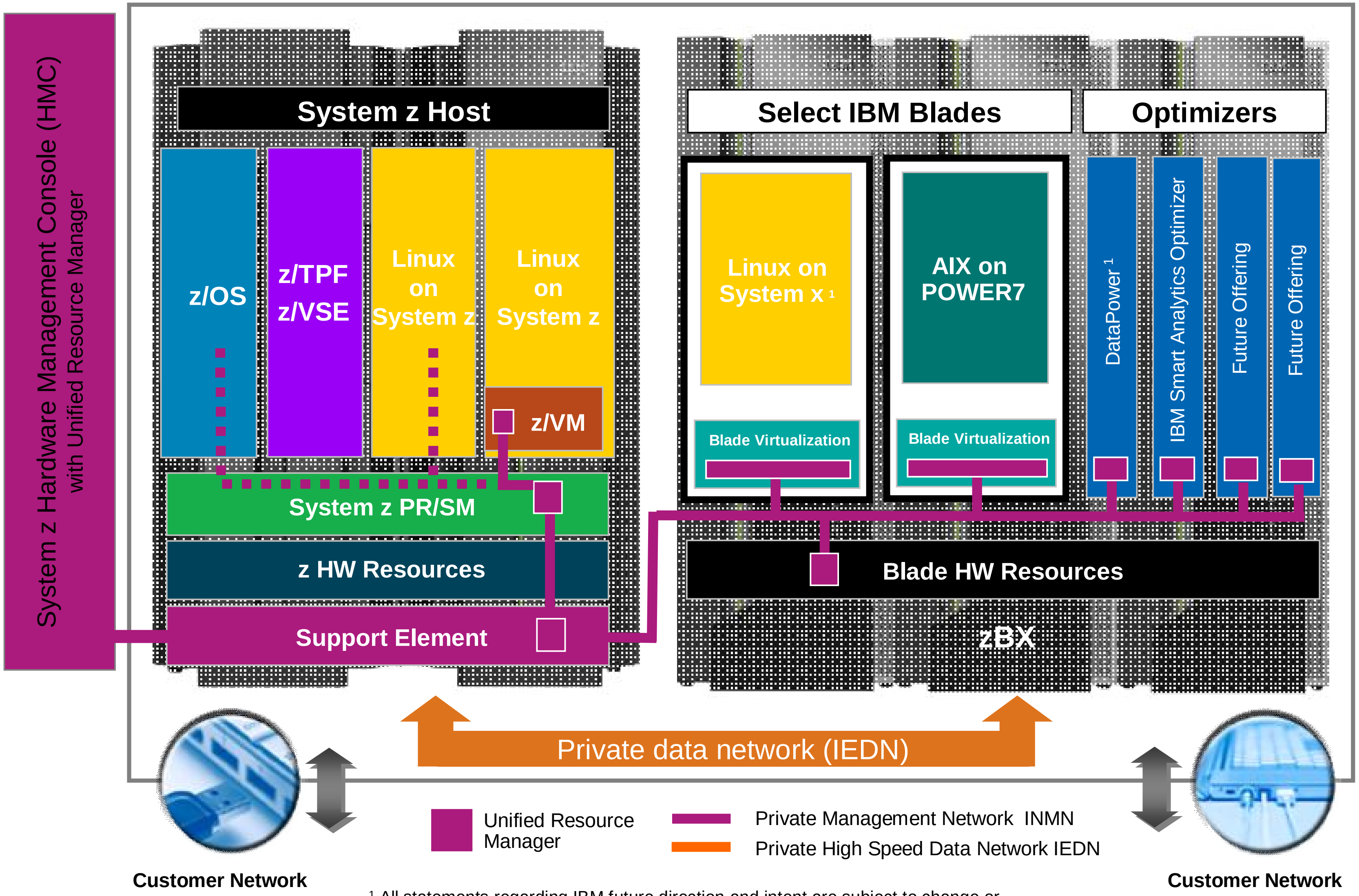




Large Tenants	Medium Tenants	Small Tenants
Isolation: Databases	Isolation: Tables	Isolation: Rows
Shared: Hardware	Shared: Database	Shared: Tables

Putting zEnterprise System to the task

Use the smarter solution to improve your application design

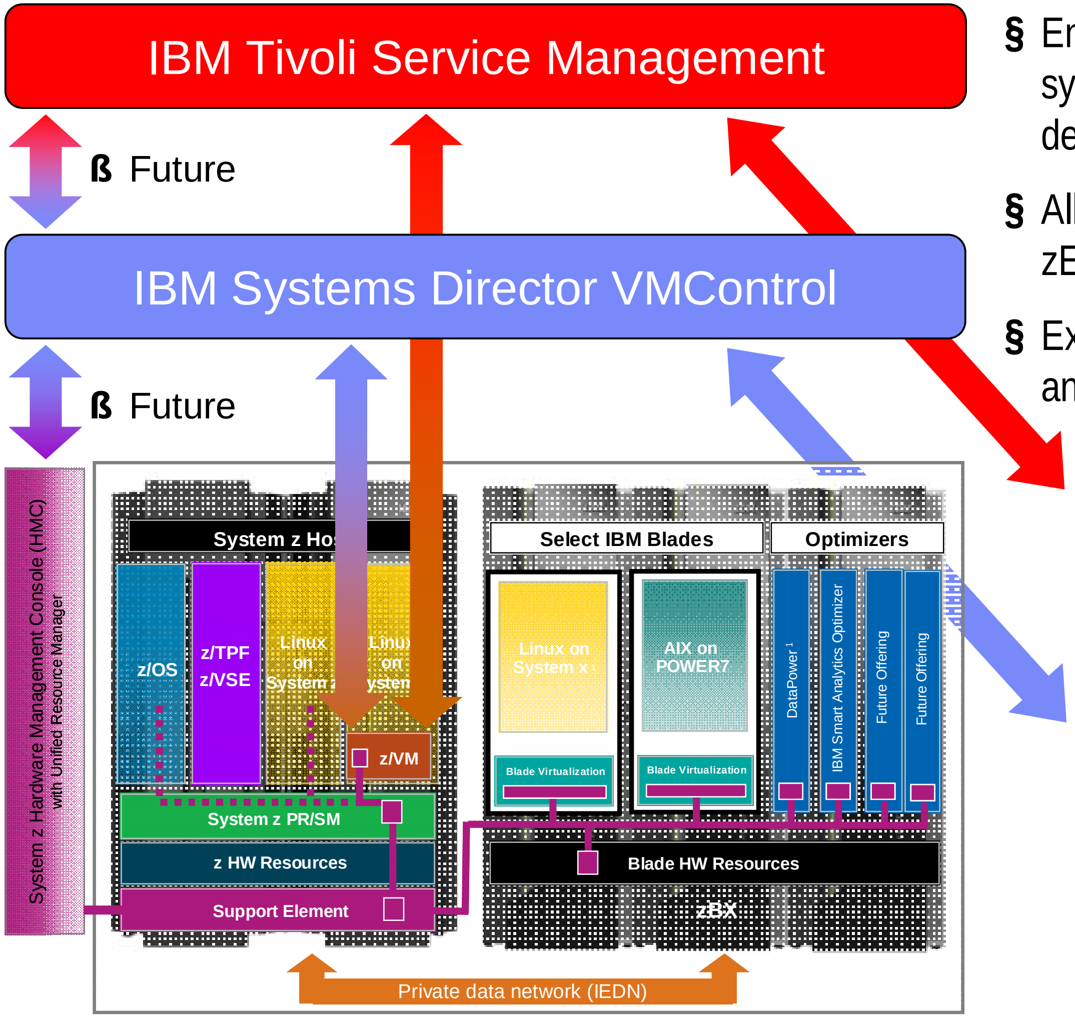


■	Unified Resource Manager	▬	Private Management Network INMN
		▬	Private High Speed Data Network IEDN

[1] All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represents goals and objectives only.

Multi-System Cloud Management on IBM zEnterprise

The Big Picture Going Forward



- Enables optimal workload placement in a multi-system cloud infrastructure: spend less *and* deliver higher qualities of service
- Allows clients to manage all the hypervisors in a zEnterprise system with consistency
- Extends same management capabilities to Power and System x servers elsewhere in the enterprise

Note: All statements regarding IBM's plans, directions, and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Securing Your Cloud with **IBM Tivoli Security for zEnterprise**

ü Enforce security policy compliance and reduce security vulnerabilities

ü Centrally manage and protect access to applications, business services, infrastructure, and data

ü Leverage the mainframe as your Enterprise Security Hub for cross-platform security

Tivoli zSecure suite and Tivoli Security Management for z/OS

§ Cost-effective security administration, security policy enforcement, automated auditing and compliance to detect threats and reduce risk

Tivoli zSecure Manager for RACF z/VM

§ Mainframe audit solution for the enterprise security hub for analysis and reporting

§ Mainframe administration enables efficient and effective RACF administration

Tivoli zSecure suite
Tivoli zSecure Manager for RACF z/VM
Tivoli zSecure Audit*
Tivoli zSecure Admin
Tivoli zSecure Alert**
Tivoli zSecure Visual
Tivoli zSecure Command Verifier
Tivoli zSecure CICS Toolkit
RACF
z/VM
z/OS

*Also available for ACF2™ and Top Secret®
**Also available for ACF2

Tivoli Federated Identity Manager

§ Secure information sharing with federated SSO and a security token service

§ New-user self enrollment capabilities

Tivoli Access Manager Family

§ Data-level entitlement management and enforcement

§ B2C enrollment and proxy standards

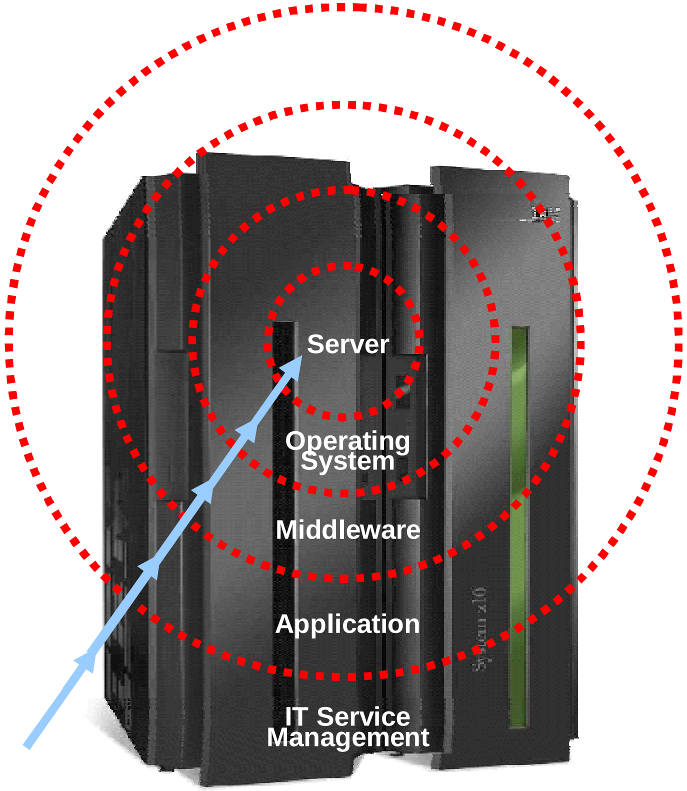
§ Federation standards for on- and off-premise

Summary

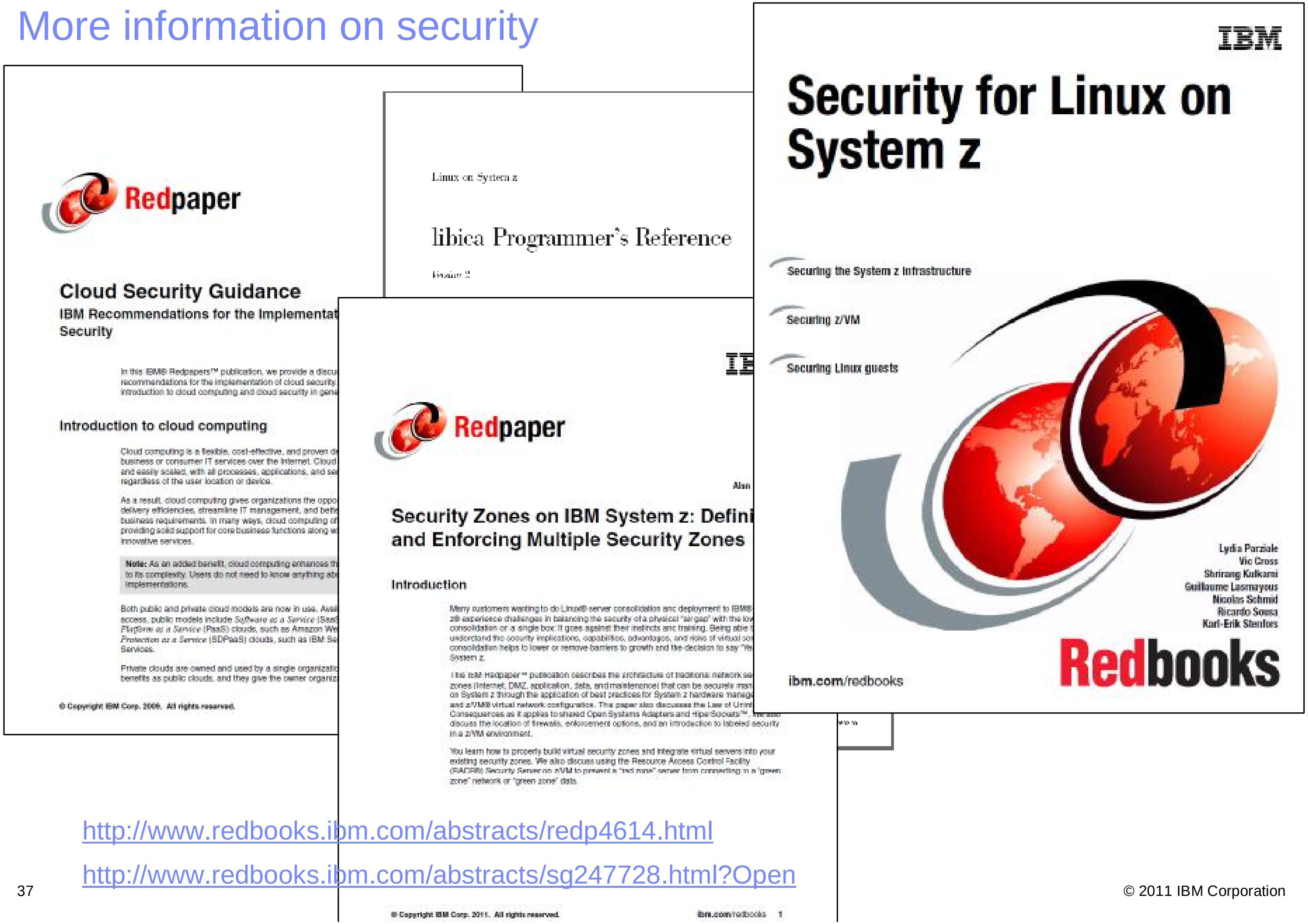
- Security is more than a “Perimeter” defence”
  - a firewall alone is not sufficient

- Security begins with the security capabilities / functions available within the Enterprise infrastructure

- Linux running on System z leverages:
  - Unique hardware features
  - Support for trusted cryptography algorithms
  - Secure open source implementation
  - A software layer to make use of the HW functionality from the application layer



More information on security



Redpaper

Cloud Security Guidance

IBM Recommendations for the Implementat
Security

In this IBM® Redpapers™ publication, we provide a discu
recommendations for the implementation of cloud security.
introduction to cloud computing and cloud security in gene

Introduction to cloud computing

Cloud computing is a flexible, cost-effective, and proven de
business or consumer IT services over the Internet. Cloud
and easily scaled, with all processes, applications, and se
regardless of the user location or device.

As a result, cloud computing gives organizations the oppo
delivery efficiencies, streamline IT management, and bette
business requirements. In many ways, cloud computing of
providing solid support for core business functions along w
innovative services.

Note: As an added benefit, cloud computing enhances th
to its complexity. Users do not need to know anything ab
implementations.

Both public and private cloud models are now in use. Avail
access, public models include *Software as a Service* (SaaS
Platform as a Service (PaaS) clouds, such as Amazon We
Protection as a Service (SDPaaS) clouds, such as IBM Se
Services.

Private clouds are owned and used by a single organizatio
benefits as public clouds, and they give the owner organiz

© Copyright IBM Corp. 2009. All rights reserved.

Linux on System z

libica Programmer's Reference

Version 2

IBM

Redpaper

Alan

Security Zones on IBM System z: Defini
and Enforcing Multiple Security Zones

Introduction

Many customers wanting to do Linux® server consolidation and deployment to IBM®
z® experience challenges in balancing the security of a physical "air gap" with the low
consolidation or a single box: It goes against their instincts and training. Being able t
understand the security implications, capabilities, advantages, and risks of virtual ser
consolidation helps to lower or remove barriers to growth and the decision to say "Ye
System z.

This IBM Redpaper™ publication describes the architecture of traditional network se
zones (Internet, DMZ, application, data, and maintenance) that can be securely man
on System z through the application of best practices for System z hardware manage
and z/VM® virtual network configuration. This paper also discusses the Law of Unint
Consequences as it applies to shared Open Systems Adapters and HiperSockets™. We also
discuss the location of firewalls, enforcement options, and an introduction to labeled security
in a z/VM environment.

You learn how to properly build virtual security zones and integrate virtual servers into your
existing security zones. We also discuss using the Resource Access Control Facility
(RACF®) Security Server on z/VM to prevent a "red zone" server from connecting to a "green
zone" network or "green zone" data.

© Copyright IBM Corp. 2011. All rights reserved. ibm.com/redbooks 1

IBM

Security for Linux on System z

Securing the System z Infrastructure

Securing z/VM

Securing Linux guests

Lydia Parziale
Vic Cross
Shrirang Kulkarni
Guillaume Lasmayous
Nicolas Schmid
Ricardo Sousa
Karl-Erik Stenfors

ibm.com/redbooks

Redbooks

http://www.redbooks.ibm.com/abstracts/redp4614.html

http://www.redbooks.ibm.com/abstracts/sg247728.html?Open

धन्यवाद

Hindi

多謝

Traditional Chinese

ขอบคุณ

Thai

Спасибо

Russian

Bedankt

Nederlands

Thank You

شكراً

Arabic

Merci

French

Obrigado

Brazilian Portuguese

Gracias!

Spanish

多谢

Simplified Chinese

Danke

German

நன்றி

Tamil

ありがとうございました

Japanese

감사합니다

Notices

This information was developed for products and services offered in the U.S.A.

Note to U.S. Government Users Restricted Rights — Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to: IBM Director of Licensing, IBM Corporation, North Castle Drive Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Trademarks

§ This presentation contains trade-marked IBM products and technologies. Refer to the following Web site:

http://www.ibm.com/legal/copytrade.shtml