Security and Virtualization - Across the Enterprise Dynamic Infrastructure and Public and Private Clouds

The future runs on System z

Jim Porell
IBM Distinguished Engineer
IBM System z Business Development

© 2009 IBM Corporation

Server Architecture Genetics

Consider the Heritage of Today's Server Platforms

- **x86 systems**
  - Key value proposition: *end-user autonomy*
  - "Ctl-Alt-Del" not a problem for a single-user system
- **UNIX systems**
  - Key value proposition: *processor speed*
  - Sweet spot: engineering/scientific computing
- **Mainframe systems**
  - Key value proposition: *mixed workloads*
  - Highest degrees of efficiency, availability, workload mgmt, security

Virtualization Essentials

Virtualization technology can be significantly constrained or compromised by the underlying system architecture.

© 2009 IBM Corporation

Extreme Virtualization with System z
Understanding the Value Proposition

- **Business pain points addressed by server virtualization:**
  - Underutilized IT assets
  - Environmental costs
  - Linear software costs per server image
  - Staff inefficiencies managing multiple real servers
  - Spiraling people costs
- **x86 virtualization pain points addressed by System z**
  - Virtual server workload management
  - Reliable high-bandwidth I/O virtualization
  - Virtual server and total system performance reporting and planning
  - Virtual server reconfiguration outages
  - Virtual machine security and integrity
  - Server sprawl with added complexity

Clients need to develop an enterprise-wide virtualization strategy that leverages the strengths of mainframe virtualization

© 2009 IBM Corporation

Virtualization and Security *Should IT Managers Be Concerned?*

Virtualization security risks being overlooked, Gartner warns

Gartner raises warning on virtualization and security.

Companies in a rush to deploy virtualization technologies for server consolidation efforts could wind up overlooking many security issues and exposing themselves to risks, warns research firm Gartner.

"Virtualization, as with any emerging technology, will be the target of new security threats," said Neil MacDonald, a vice president at Gartner, in a published statement.

– NetworkWorld.com, April 6, 2007

Posted September 21, 2007 at http://blogs.iss.net/archive/virtblog.html

"It is clear that with the increase in popularity, relevance and deployment of virtualization starting in 2006, vulnerability discovery energies have increasingly focused on finding ways to exploit virtualization technologies."

"...in a virtual environment all your exploitation risks are now consolidated into one physical target where exploiting one system could potentially allow access and control of multiple systems on that server (or the server itself). In total, this adds up to a more complex and risky security environment."

Known vulnerabilities across all of VMware's products*

VMware Vulns by Year	Total Vulns	High Risk Vulns	Remote Vulns	Vulns in 1st Party Code	Vulns in 3rd Party Code
Vulns in 2003	9	5	5	5	4
Vulns in 2004	4	2	0	2	2
Vulns in 2005	10	5	5	4	6
Vulns in 2006	38	13	27	10	28
Vulns in 2007	34	18	19	22	12

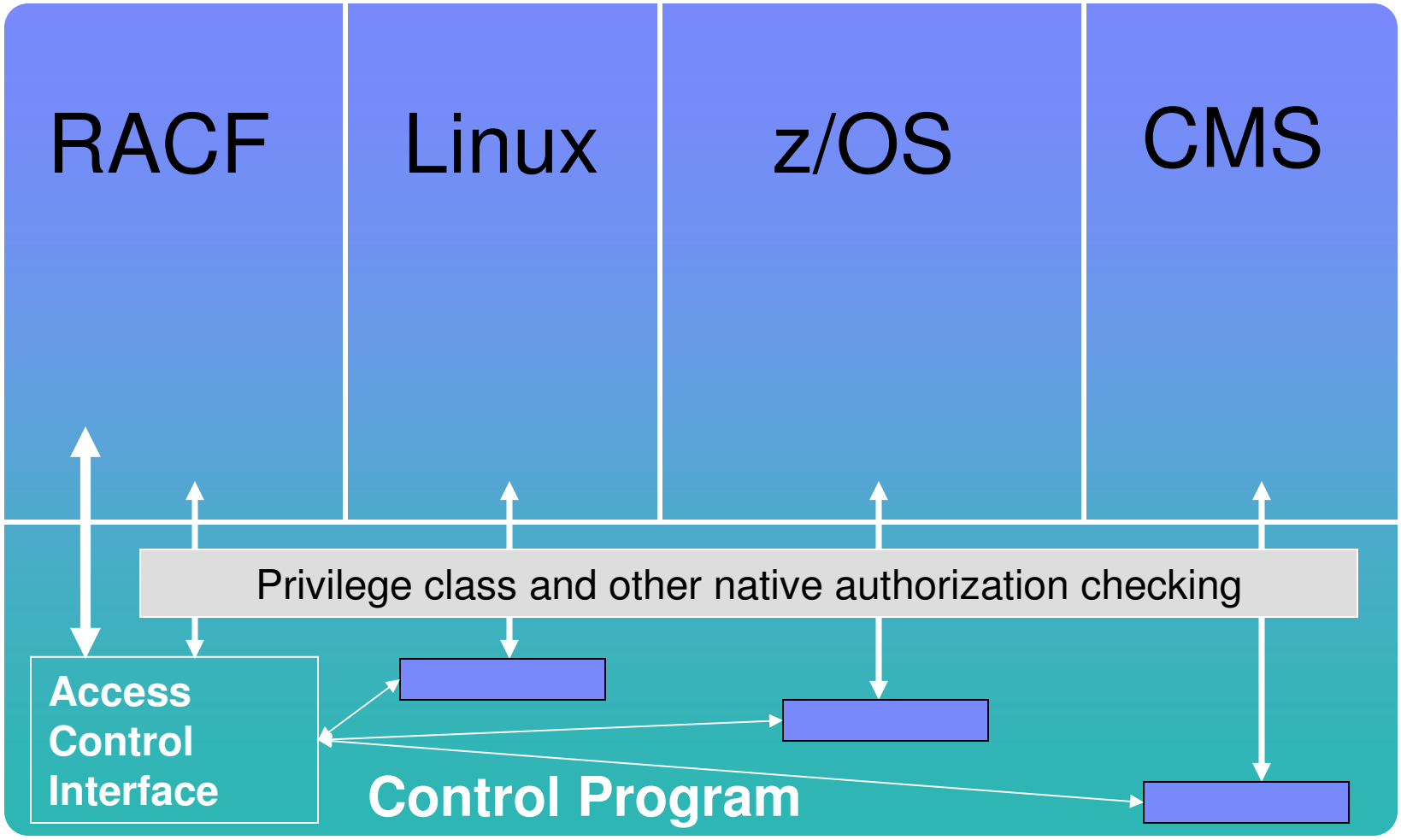
© 2009 IBM Corporation

Virtualization & Security Topics

Adding Virtualization to:		Virtualization Attributes:
People and Identity		Integrity
Applications and processes		Compartmentalization – guest/partition and multi level security
Data and information		Operational and process model changes
Network		TCO benefits with risk mitigation
Risk and Compliance		Certifications and branding – today and emerging
Competitive posture		

© 2009 IBM Corporation

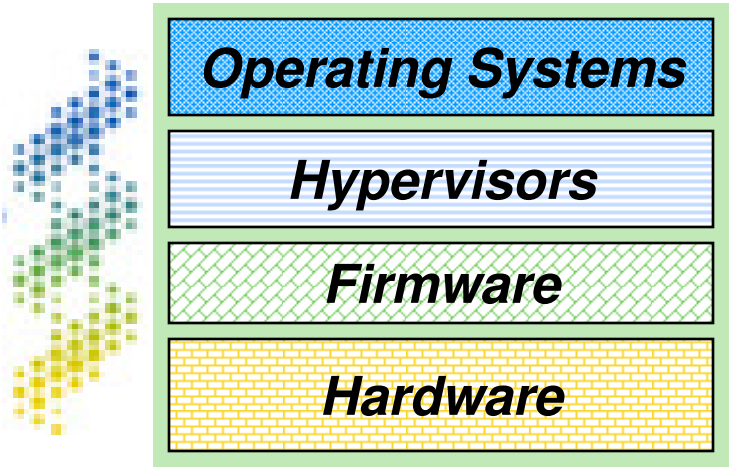
z/VM Security Architecture



© 2009 IBM Corporation

IBM System z Virtualization Genetics

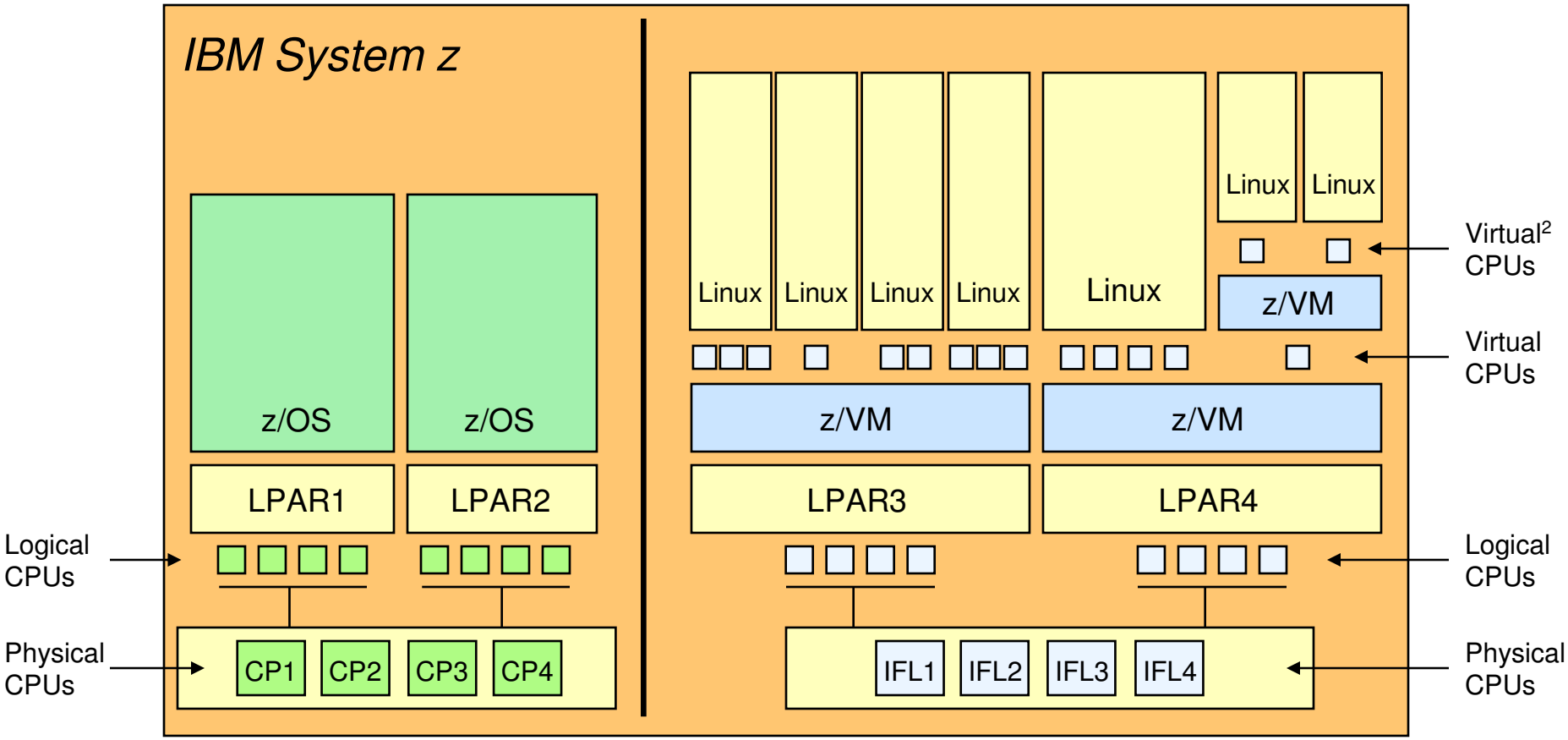
- **System z is *thoroughly* architected to host applications in a virtualized environment**
- **This is accomplished with a coordinated set of investments that permeate the technology stack of *hardware*, *firmware*, *hypervisors*, and *operating systems***
- **This means clients can maximize the utilization, scalability, and security of all system assets, including:**
  - *CPU*
  - *Memory*
  - *I/O*
  - *Networking*
  - *Cryptography*
- **All with exceptional levels of operational ease and cost efficiencies**



© 2009 IBM Corporation

IBM System z Virtualization Leadership

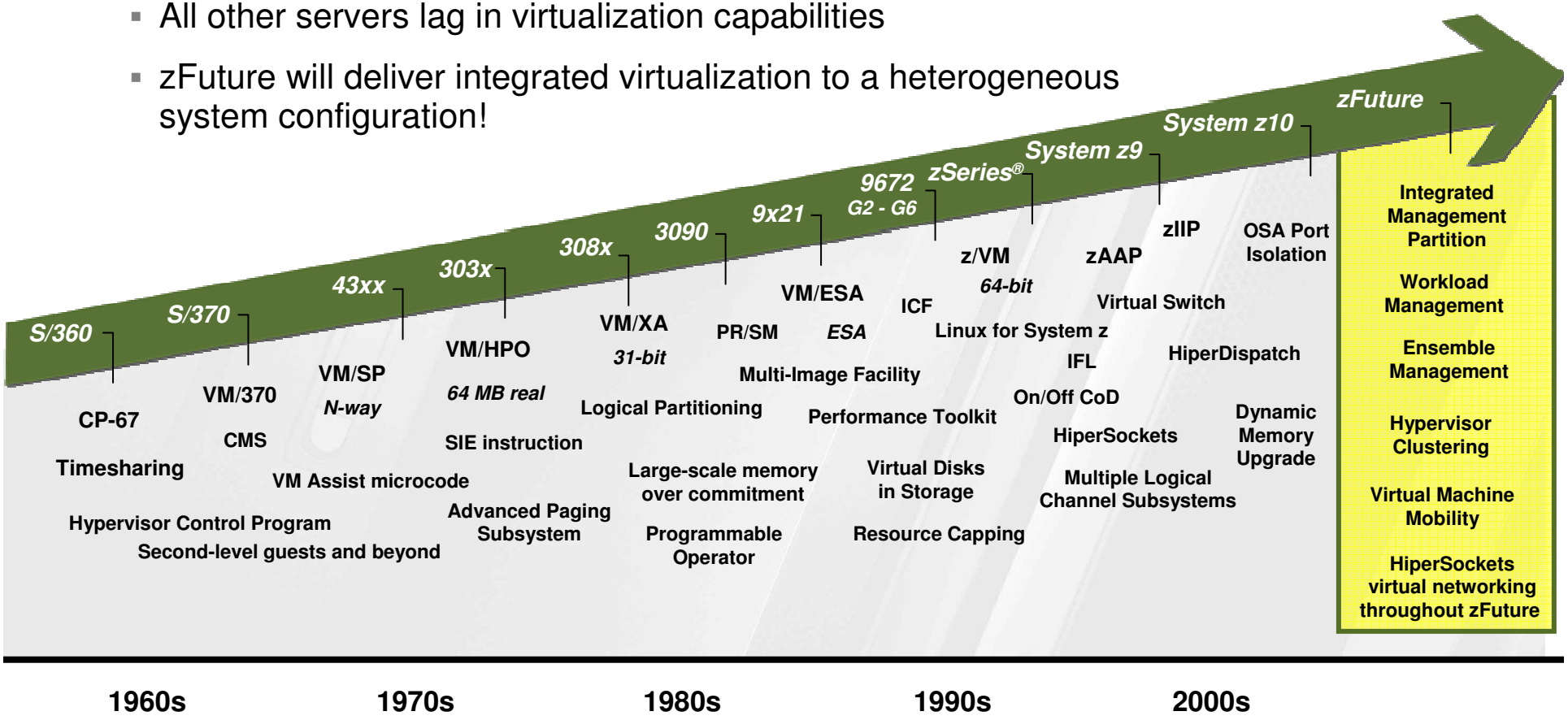
Extreme Levels of CPU Sharing



© 2009 IBM Corporation

zFuture: The next leap in virtualization

- Virtualization was pioneered and perfected on IBM mainframes
- System z continues to set the gold standard in virtualization
- All other servers lag in virtualization capabilities
- zFuture will deliver integrated virtualization to a heterogeneous system configuration!



© 2009 IBM Corporation

Tooling

Assemble Solution

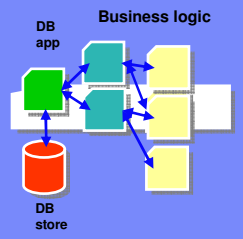


Image Library

Service Lifecycle Management

Deployment Planning

- Service Composition
- Determine required infrastructure resource configuration and capacity

Deployment, Image Mgmt

- Determine the optimal placement of service workloads
- Deployment of composite services, applications, images

Configuration, Security & Policy

- Creation of Service Availability, Performance, Security, Energy Management Policies

Visualize, Monitor

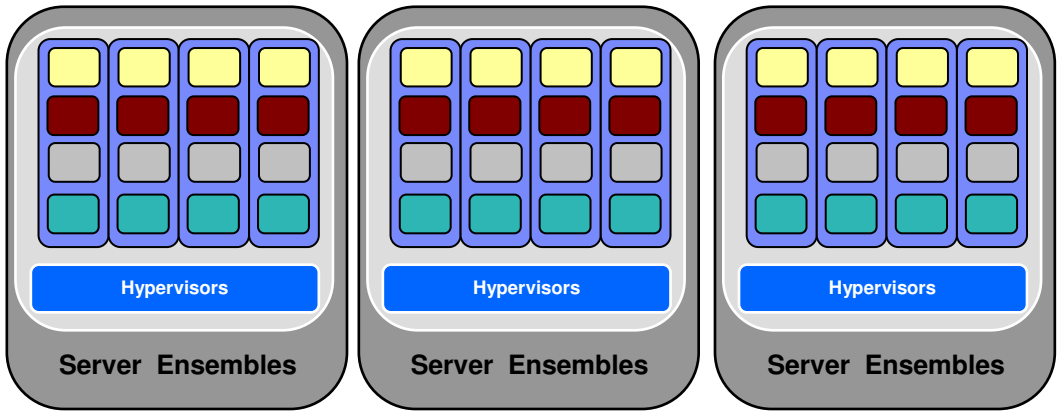
- Business System Dashboards
- Service Monitoring and Reporting

Service Management

Ensemble Management Interfaces

Ensemble Management

System z Ensemble | **Power Systems® Ensemble** | **System x® Ensemble**



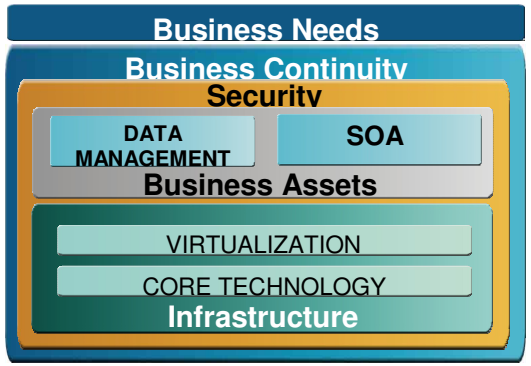
Ensemble Management

- Hardware Configuration and Operational Control
- Pooling and virtualization of server, storage, network)
- Platform Task Automation
- Autonomic resource management
- Virtual Image Management
- Energy Management
- Performance Monitoring and Management
- Availability Monitoring and Management
- Accelerator “Firmware” Configuration
- Virtual Network Configuration and Security

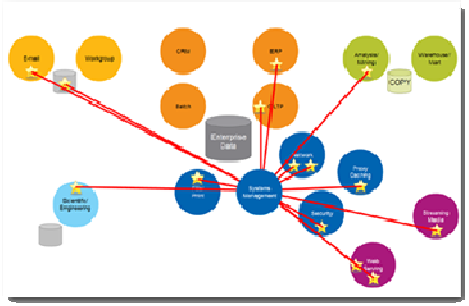
System z ensemble

System z Future

System z Mainframe



Integrated Systems Management firmware



- Integrate, monitor, and manage multi-OS resources as a single, logical virtualized system
- Single WLM, Security, and System Management interface across all resources

Accelerators

- Extend and accelerate System z workloads
- Lower cost per transaction while improving application response time for CPU intensive applications

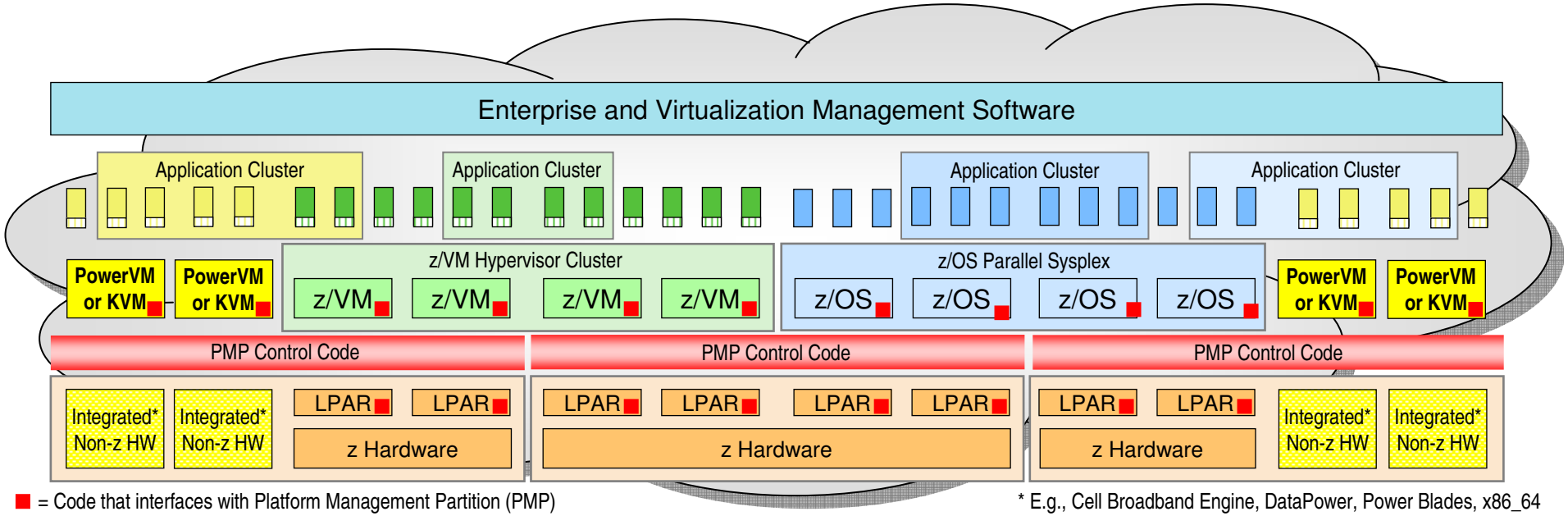
Application Serving Blades

- Logical device integration between System z resources and application serving commodity devices
- Providing competitive price-performance and improved QoS for applications with a close affinity to mainframe data

© 2009 IBM Corporation

IBM multi-architecture virtualization – Conceptual view
System z multi-system, federated Hypervisor configurati

- The System z Platform Management Partition (PMP) will host a federation of platform management functions, including:
  - Resource monitoring
  - Workload management
  - Availability management
  - Image management
  - Energy management
- Integrates with hardware management and virtualization functions
- Controls hypervisors and management agents on blades
- Open integration to enterprise-level management software



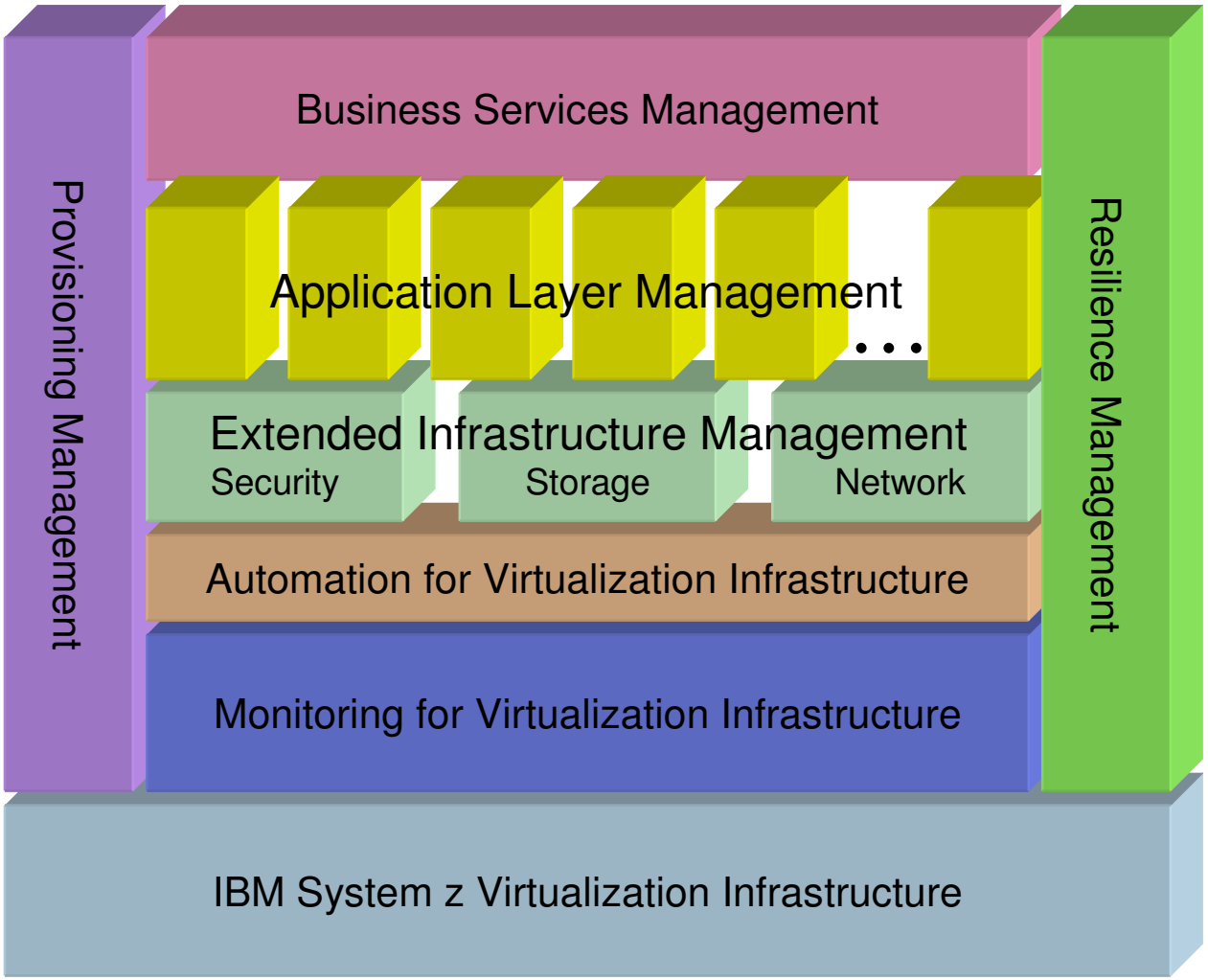
■ = Code that interfaces with Platform Management Partition (PMP)

* E.g., Cell Broadband Engine, DataPower, Power Blades, x86_64

© 2009 IBM Corporation

IBM Tivoli Virtualization Management for System z

Helping Clients Manage and Control Their Virtualized IT Infrastructure

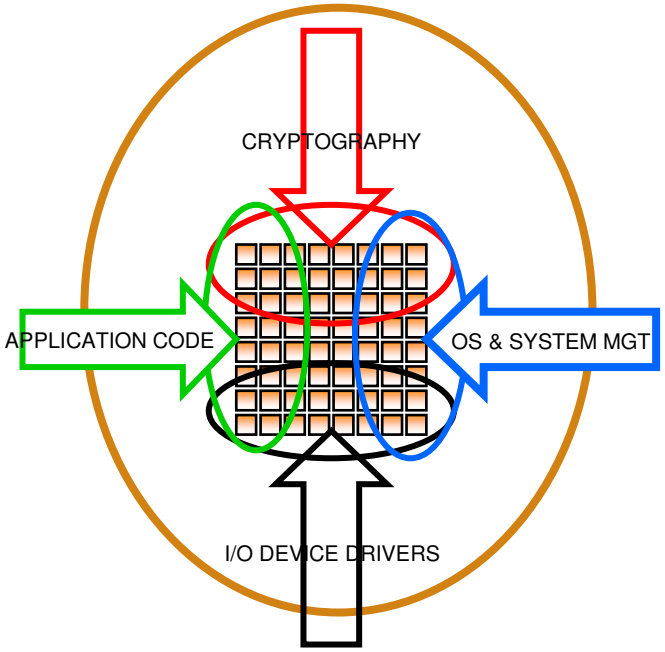


© 2009 IBM Corporation

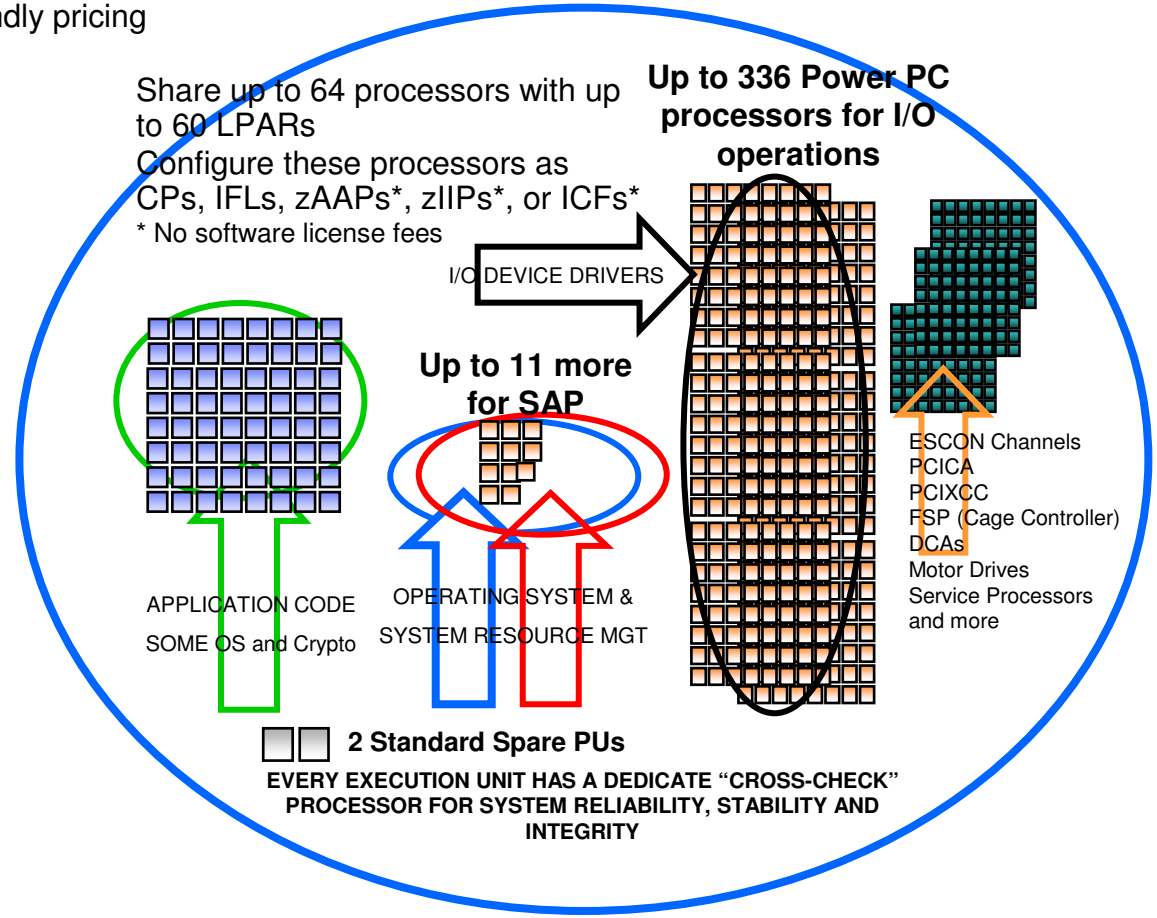
System Design Affects Virtualization Capabilities

System z packs a lot of compute power into a single box

- With TCO-friendly pricing



CPUs licensed for software do a lot other things too!



IBM System p superscalar POWER6 128-way SMP

Tuned for "Jaw-Dropping" performance on industry standard benchmarks

IBM System z10 superscalar CMOS 64-way SMP

Tuned for system utilization, industry leading RAS, system security and data integrity

And Still uses LESS ENERGY

© 2009 IBM Corporation

IBM System z: The Ultimate Virtualization Platform

- ***Virtualize*** **everything with very high levels of utilization**
  - CPU, memory, network, I/O, cryptographic features, coupling facility, ...

Consolidate all types of workloads

- ***Massively scale*** **your workload on a single System z mainframe**
  - Host tens-to-hundreds of virtual machines on z/VM
  - Each virtual machine on z/VM can access up to 24,576 devices

Smart economics: start small and grow big in the same box

- ***Non-disruptively add*** **anything**
  - Up to 64x CPU scalability per mainframe, 32x scalability per z/VM LPAR
  - z/VM is designed to support more than 1 TB of active virtual memory

Able to respond to workload spikes

- ***Security*** **for everything**
  - Highest security classification for general purpose servers
  - System z LPAR technology is EAL 5 certified

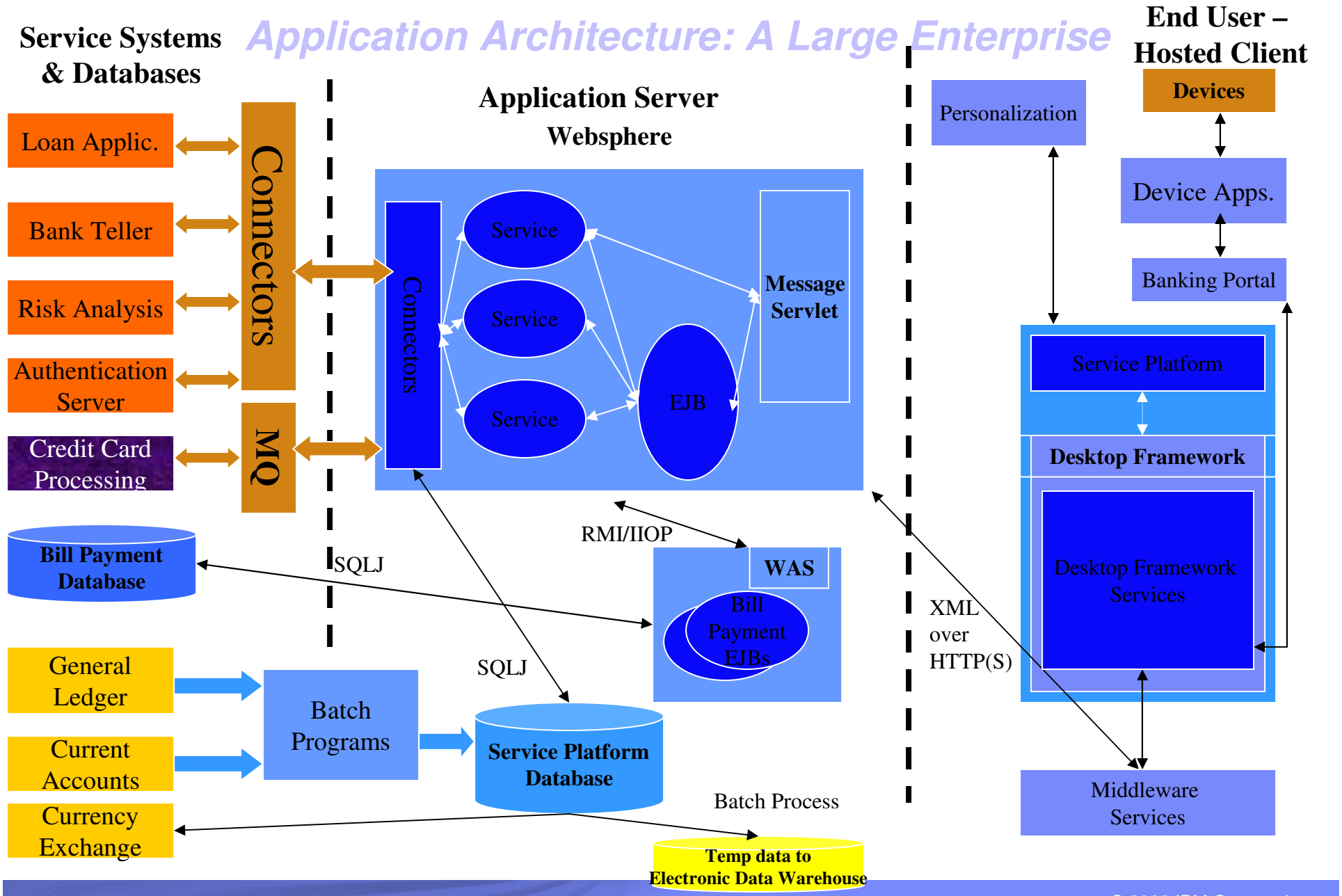
Helps secure your virtual servers and reduce business risk

- ***Optimize and integrate*** **it all with the IBM software portfolio**

Increase staff productivity and virtualize the enterprise

© 2009 IBM Corporation

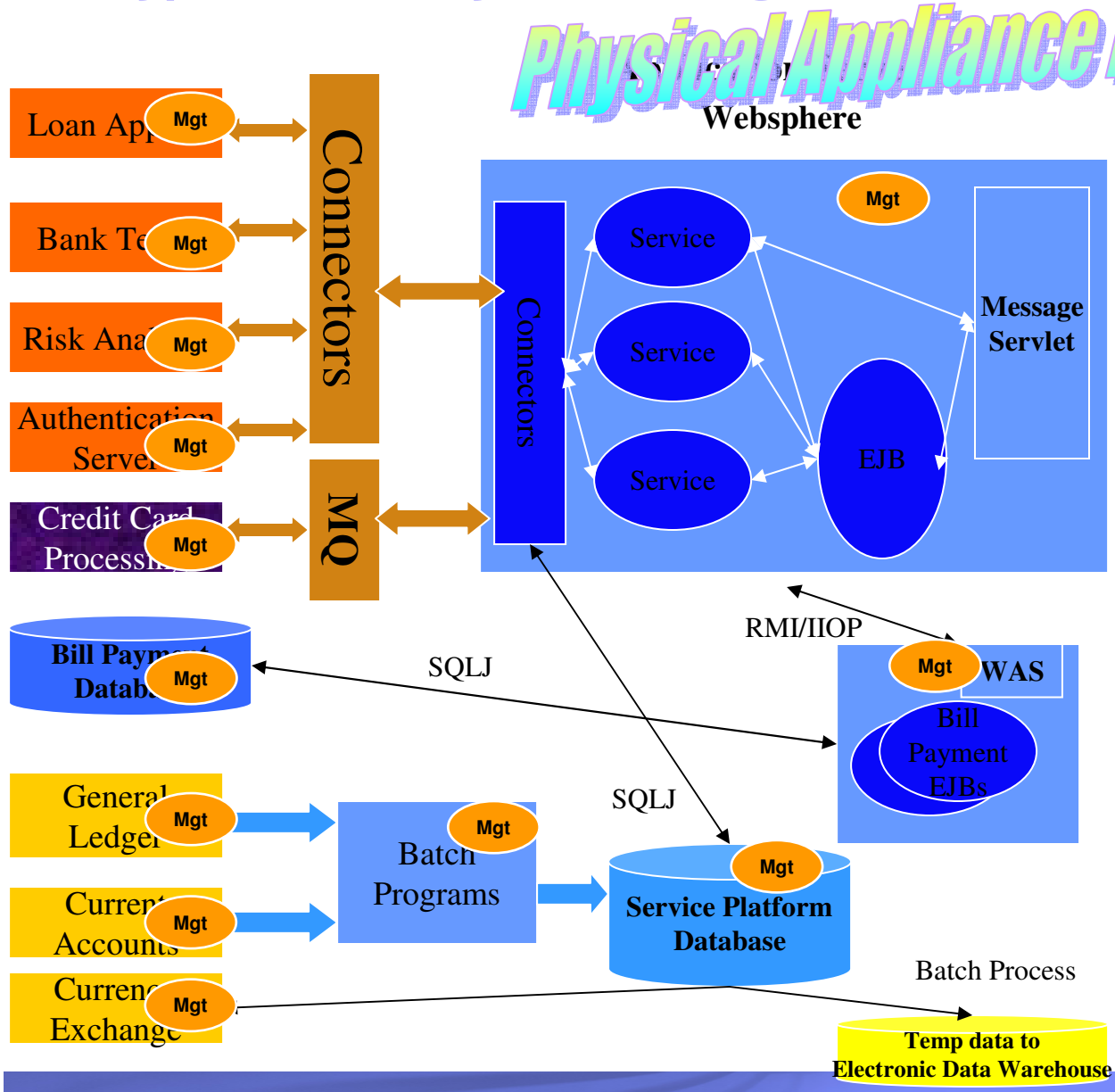
Application Architecture: A Large Enterprise



© 2009 IBM Corporation

Typical multi-system Design: Numerous Mgmt Domains

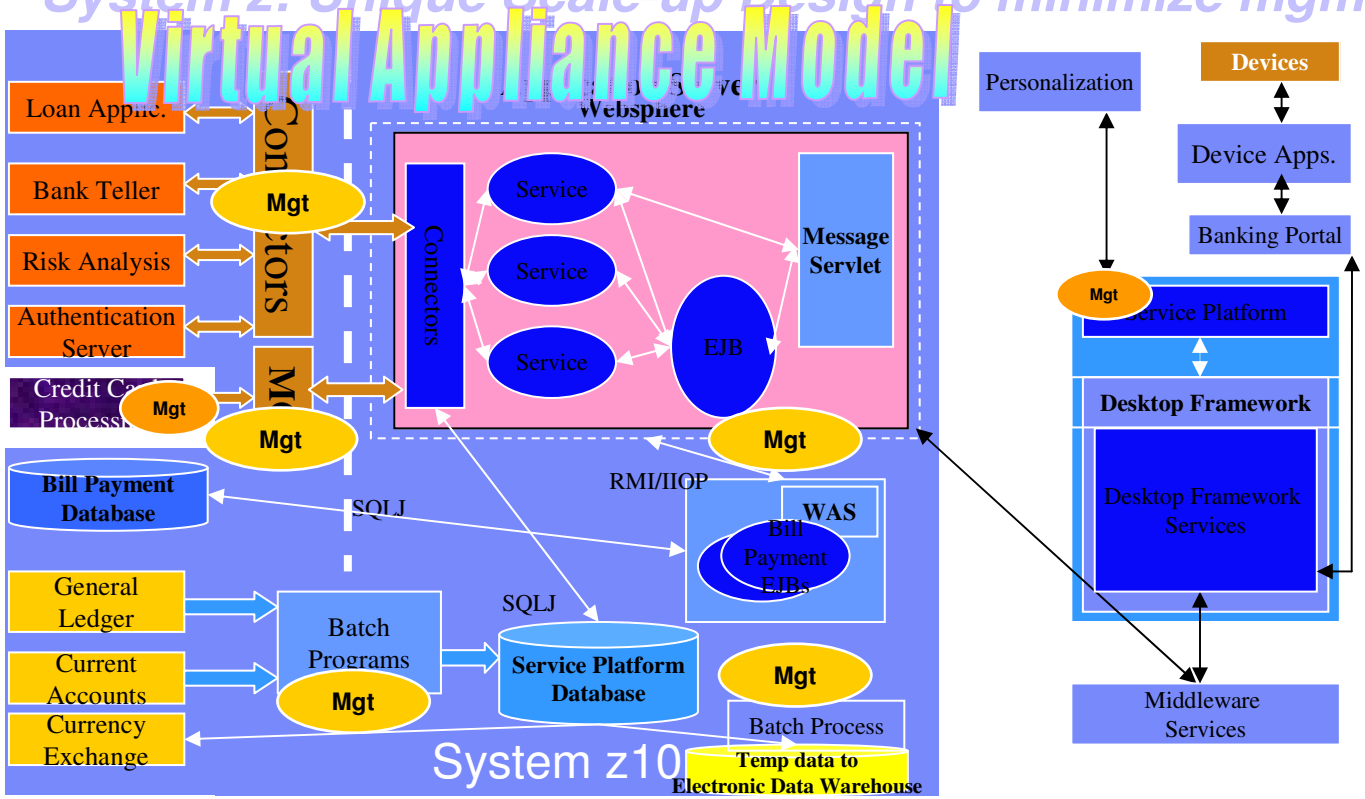
Physical Appliance Model



- Authentication
- Alert processing
- Firewalls
- Virtual Private Networks
- Network Bandwidth
- Encryption of data
- Audit Records/Reports
- Provisioning Users/Work
- Disaster Recovery plans
- Storage Management
- Data Transformations
- Application Deployment

© 2009 IBM Corporation

System z: Unique Scale-up Design to minimize mgmt domains



Potential advantages of consolidating your application and data serving

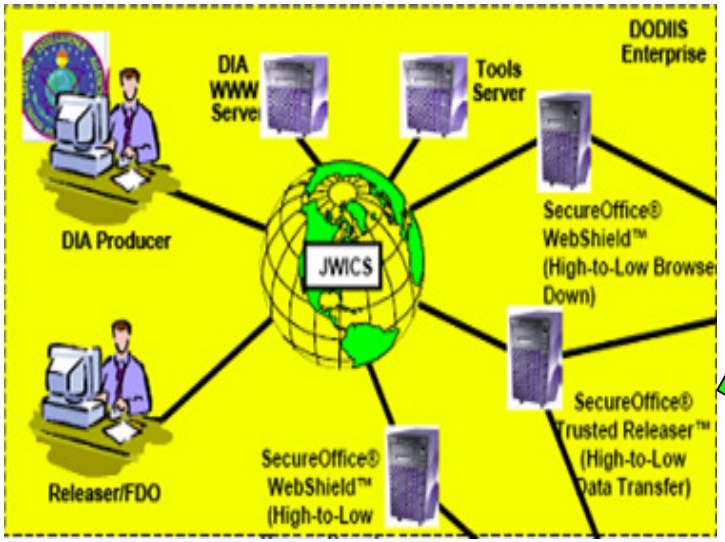
Security	Fewer points of intrusion
Resilience	Fewer Points of Failure
Performance	Avoid Network Latency
Operations	Fewer parts to manage
Environmentals	Less Hardware
Capacity Management	On Demand additions/deletions
Utilization	Efficient use of resources
Scalability	Batch and Transaction Processing
Auditability	Consistent identity
Simplification	Problem Determination/diagnosis
Transaction Integrity	Automatic recovery/rollback

With IFL

With zAAP & zIIP

© 2009 IBM Corporation

Secure Virtualization Changes Operational Model

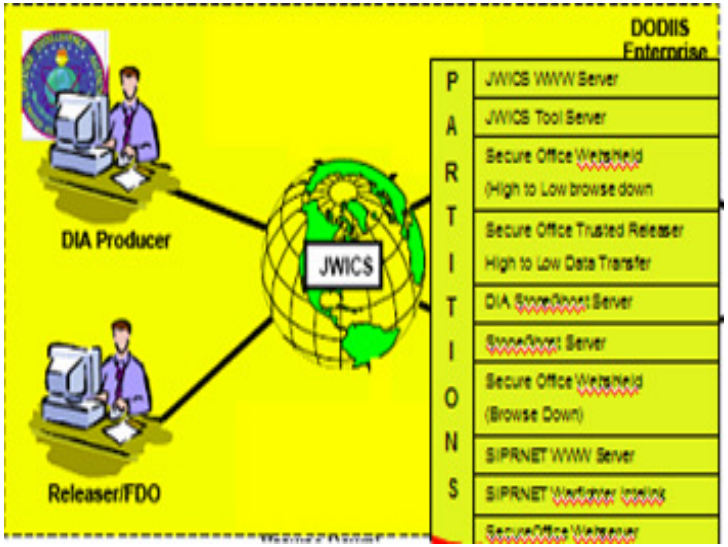


Opportunities for Cost Savings

- Overcommitment of CPU resources can reduce software license fees
- Large-scale virtual server deployment on a single z/VM hypervisor can greatly enhance staff productivity
- Reliability and redundancy of System z infrastructure helps lessen application outages
- Flexible configuration options for business continuance (e.g., Capacity Backup on Demand)
- Cost-attractive economic model for technology refreshes (e.g., specialty engines carry forward to next generation)

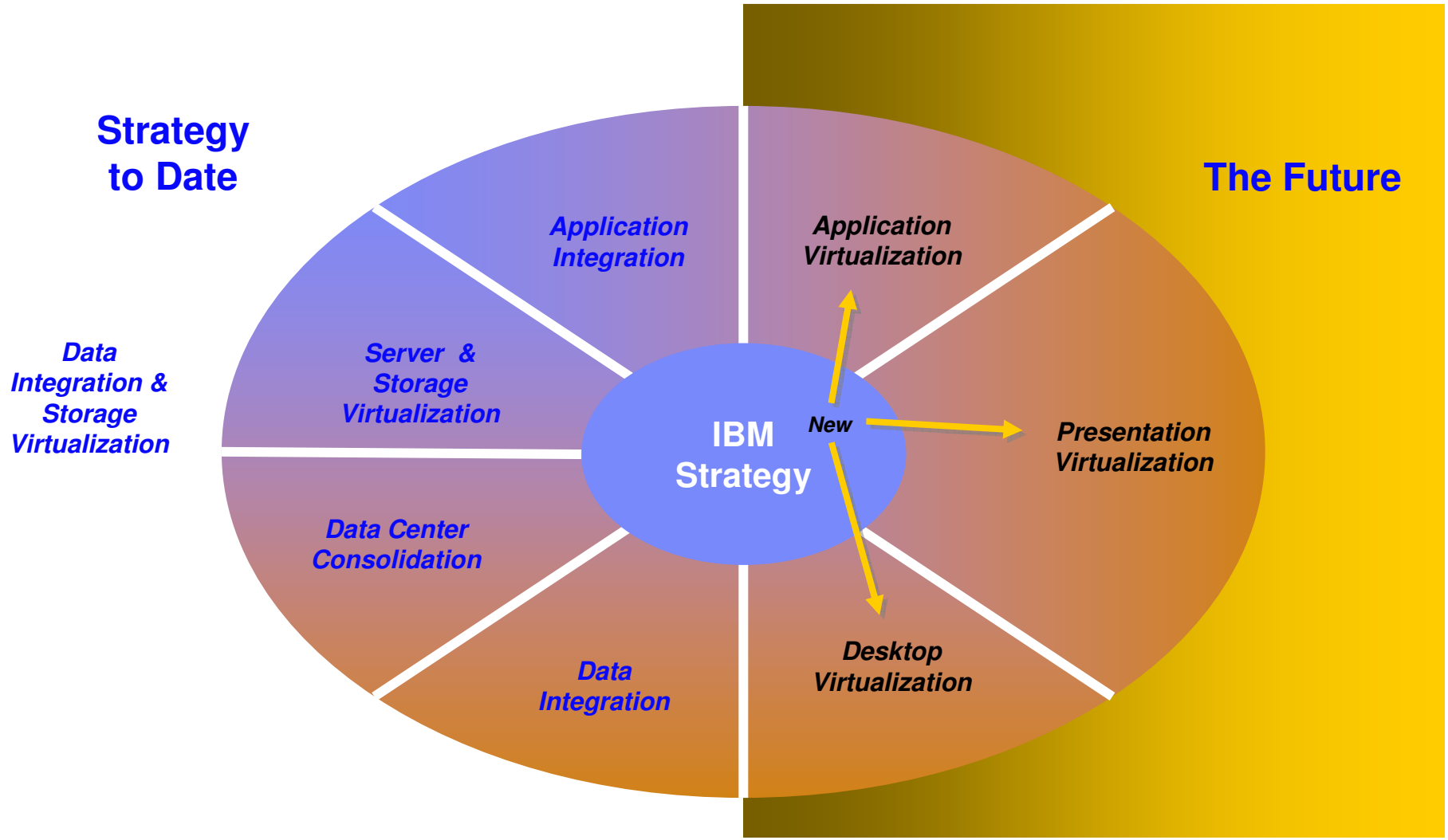
Same code, different container, superior operations

Near-linear scalability	up to 900,000+ concurrent users; TBs of data
"Mean Time Between Failure"	measured in decades versus months
¼ network equipment costs	virtual and physical connectivity
1/25th floor space	400 sq. ft. versus 10,000 sq. ft
1/20 energy requirement	$32/day versus $600/day
1/5 the administration	< 5 people versus > 25 people
Highest average resource utilization	Up to 100% versus < 15%
Capacity Management & upgrades	On demand; in hours, not weeks/months
Security intrusion points	Reduced by z architecture and # of access pts.
Higher concurrent workload	hundreds of applications versus few



© 2009 IBM Corporation

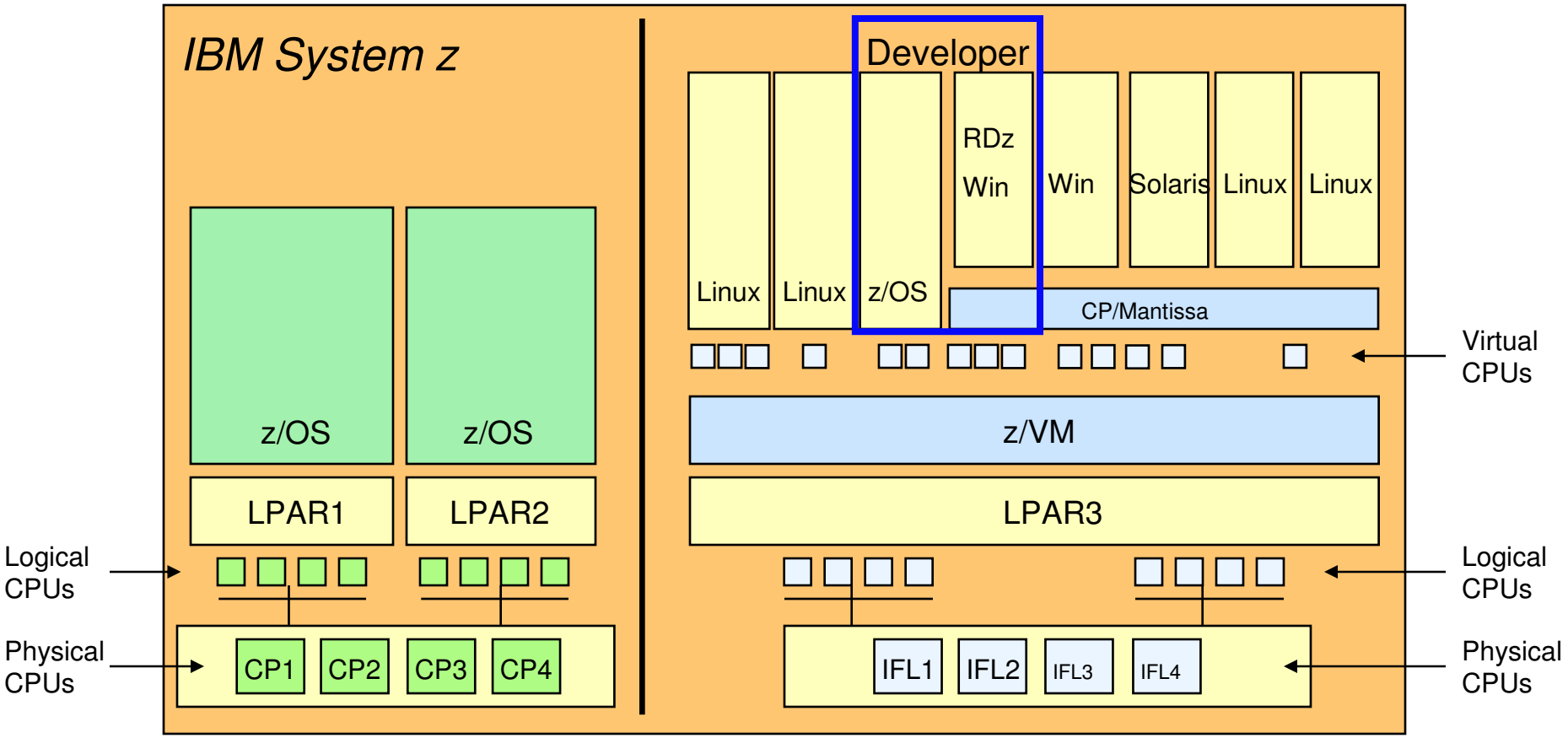
Our premise: The market is at a tipping point – with the right investment in client consolidation and virtualization, IBM can re-shape the way our customers define their security strategy (and subsequent spend)



© 2009 IBM Corporation

IBM System z Virtualization Leadership

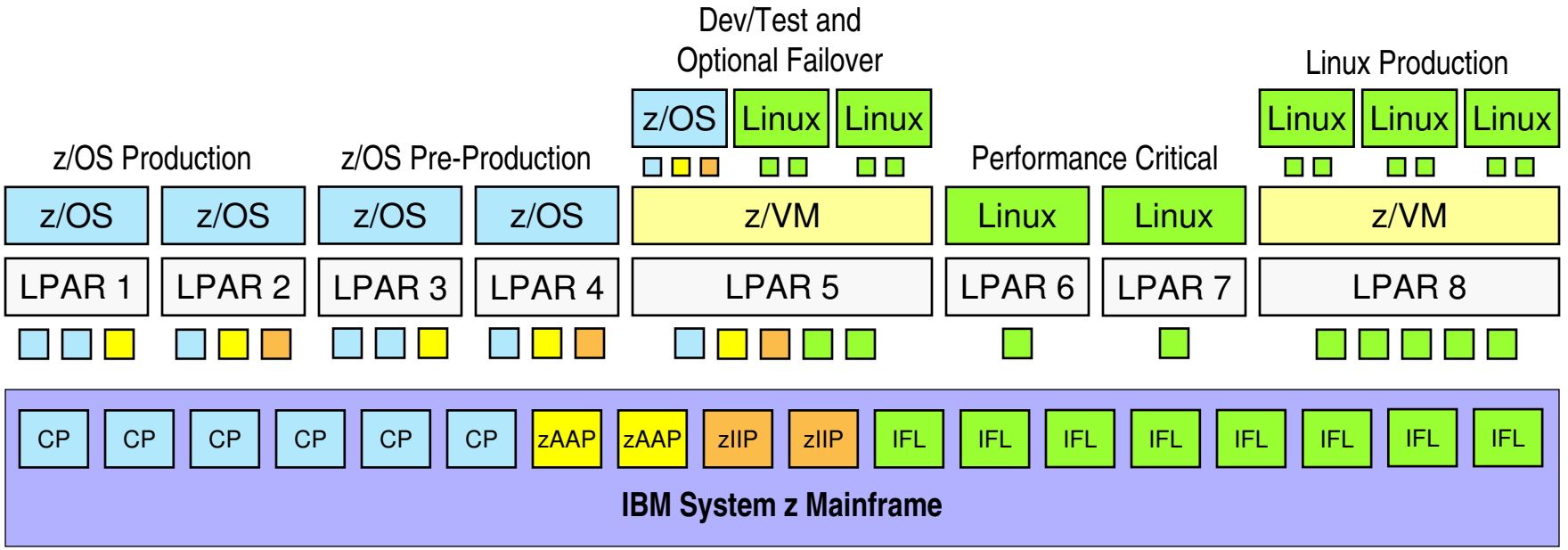
Extreme Levels of CPU Sharing - x86 emulation CONCEPT (not plan!)



© 2009 IBM Corporation

The Power and Flexibility of System z Virtualization

- Over 40 years of continuous innovation in virtualization technologies
- Multiple images concurrently share all physical resources
- Resources delivered as required, automatically, based on business-oriented goals
- New OS images can be started without affecting ongoing work
- Hardware assists used to accelerate virtualization operations (e.g., SIE)



© 2009 IBM Corporation

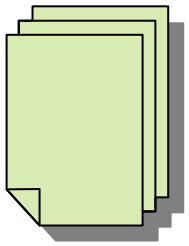
Payment Card Industry
PCI DSS Requirements "The Digital Dozen"

Build and Maintain a Secure Network	
1.	Install and maintain a firewall configuration to protect cardholder data
2.	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	
3.	Protect stored cardholder data
4.	Encrypt transmission of cardholder data sent across open, public networks
Maintain a Vulnerability Management Program	
5.	Use and regularly update anti-virus software
6.	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	
7.	Restrict access to cardholder data by business need-to-know
8.	Assign a unique ID to each person with computer access
9.	Restrict physical access to cardholder data
Regularly Monitor and Test Networks	
10.	Track and monitor all access to network resources and cardholder data
11.	Regularly test security systems and processes
Maintain an Information Security Policy	
12.	Maintain a policy that addresses information security – Connected Entities and Contracts

PCI DSS Ver. 1.1

© 2009 IBM Corporation

Security on System z: Reducing risk for the Enterprise



Basic Insurance Policy

$100,000 Liability

Rider: Excess replacement for valuable items

Rider: Excess medical coverage

Rider: Unlimited vehicle towing

Rider: Excess liability insurance $3,000,000

Basic Security: System z

RACF

Data Encryption services Enterprise Key mgt

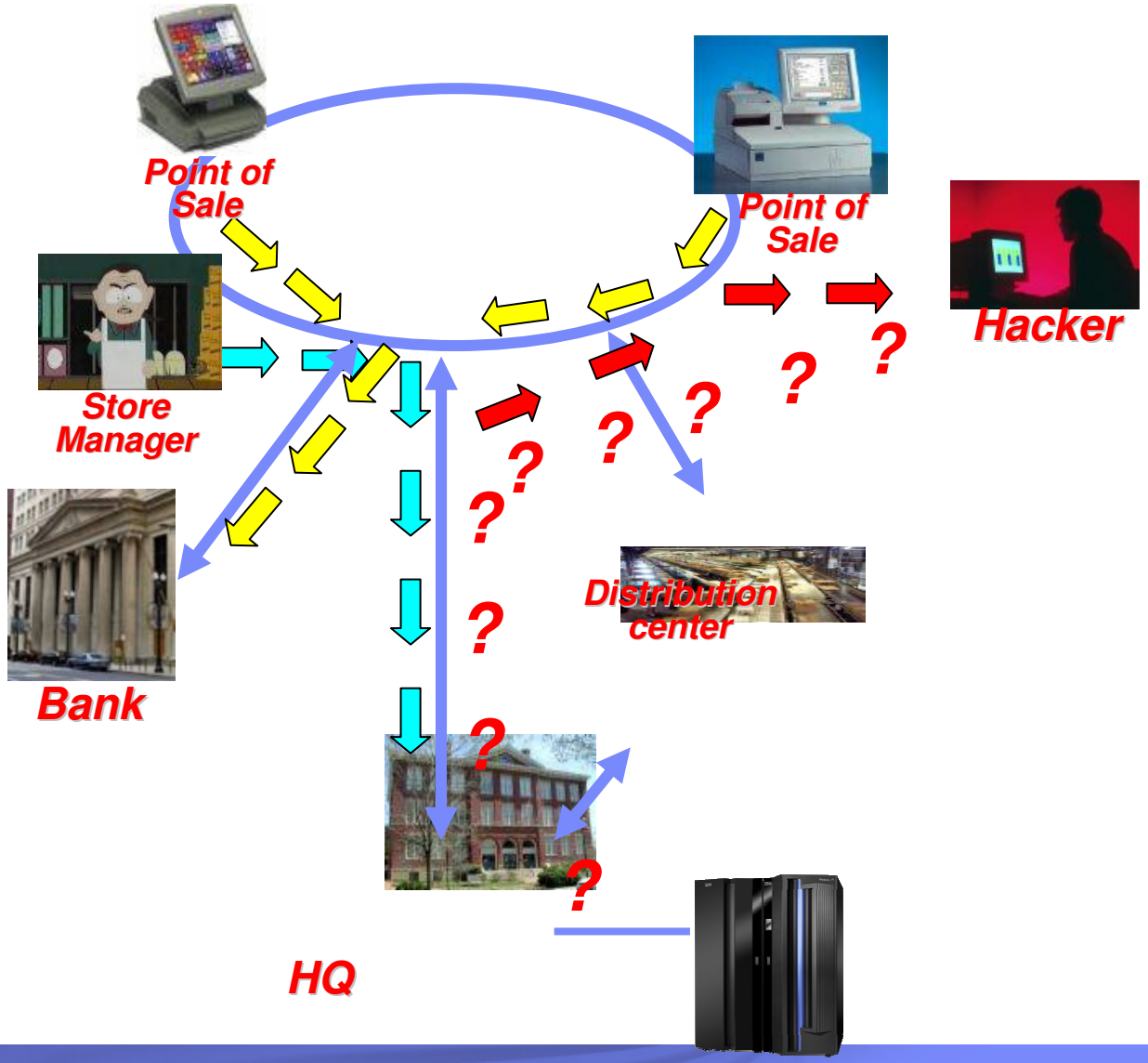
Identity Management

Compliance Reporting

Fraud Prevention, Forensics and Analytics

© 2009 IBM Corporation

Retail Customer Problem



- Store uses WEP wireless for Point of Sale devices
- POS processes cards with banks
- Common password on all store systems
- Security patches not applied to store systems
- Hacker plugs in and gets copies of all transactions
- Problem detected and store systems are getting fixed.
- Mainframe folks are happy they are bullet proof

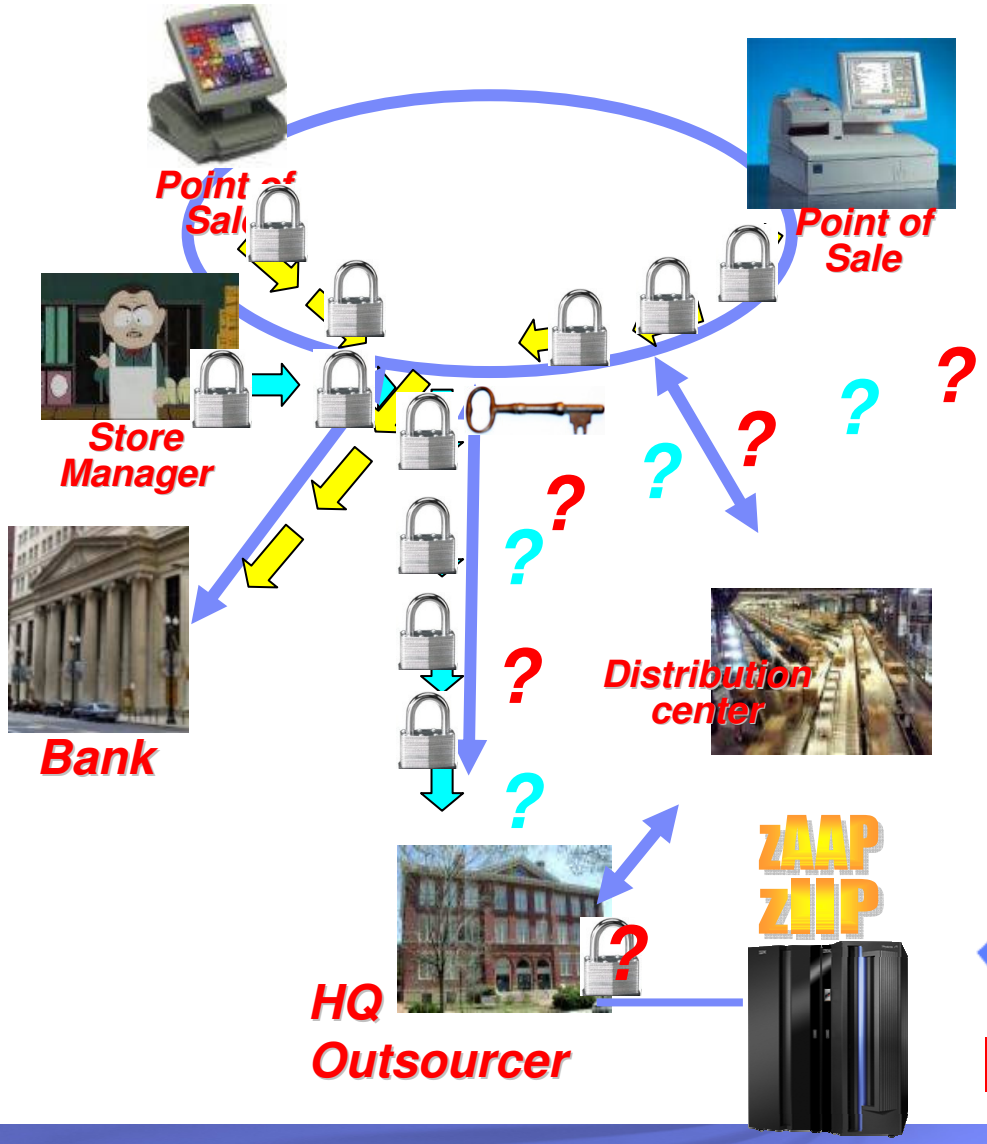
© 2009 IBM Corporation

Real World Customer Problems

- **That problem could never happen at my business**
  - **Wrong** – this problem can occur anywhere there is a change in security administrative control
- **The weakest link in an enterprise is typically the end user interface**
  - Virus, worms, Trojan Horses enable someone to hijack the end user interface
  - In turn, that hijacked desktop can be used to log into any other server
    - Is it “really the authorized end user”? Perhaps not.
      - That’s a large risk to a business.
- **Outsourcers and mainframe IT operations have SLA’s that protect the data they host on their systems.**
- **Do their customers and end users have SLA’s that specify minimum desktop security? Do they manage Desktops and mainframes together?**
  - Typically not – as a result, there is a major risk that a compromised end user interface can result in compromised mainframe access.
- **Our Goal is to look at security management across these domains**

© 2009 IBM Corporation

Examples of End to End Security



- Mainframe Userid and Password Encryption via Host on Demand
- Virtual Private Network encryption (which exploits the zIIP)
- Audit and anomaly detection via TCIM
- Fraud Forensics, Analysis and Prevention via Intellinx (which exploits the zAAP)
- LAN encryption via WPA which exploits z/OS PKI
- z/OS PKI deployment with Global Services
- PKI management via Venafi

z/OS PKI Services

IBM Global Services: Security & Privacy Consulting

VENAFI

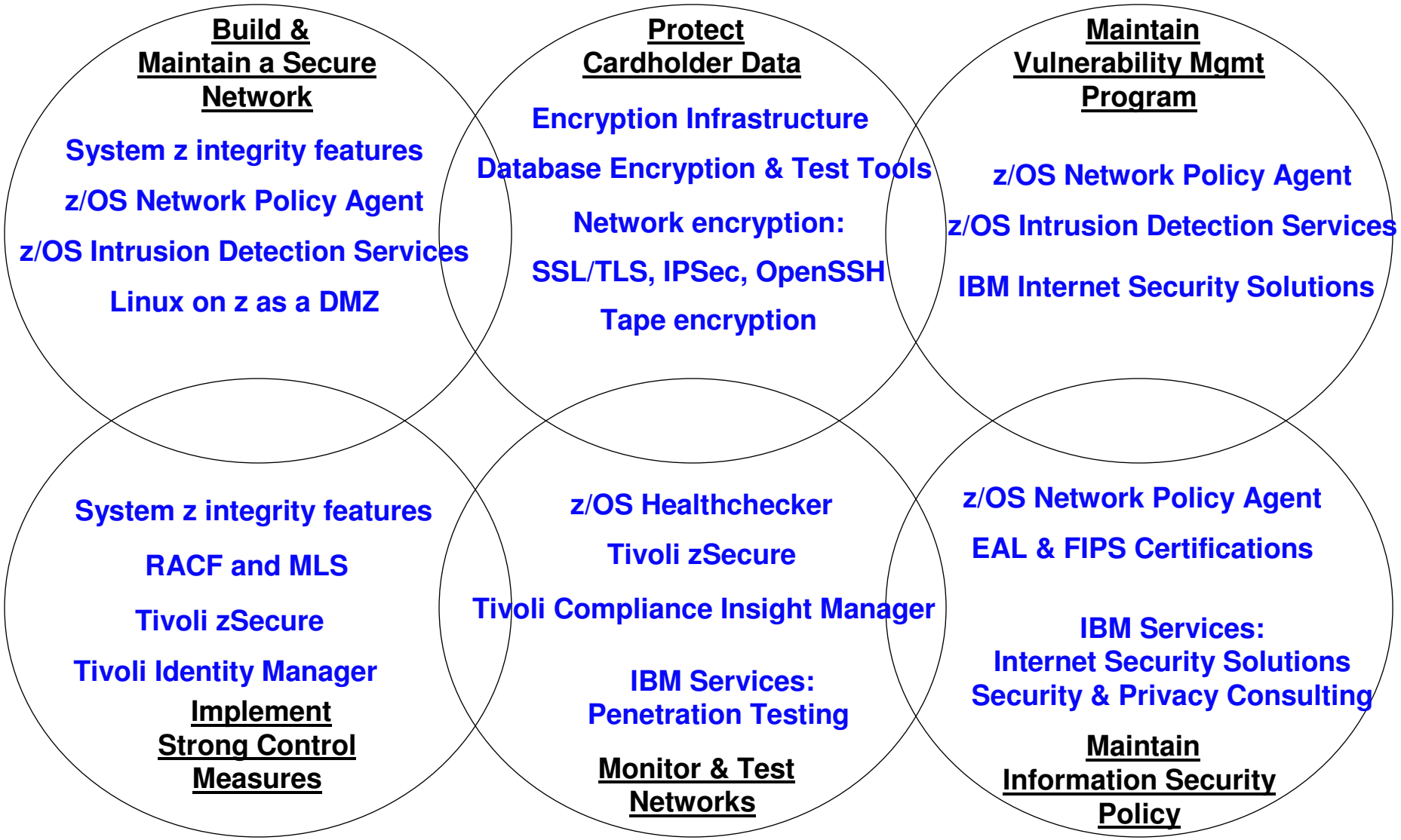
Intellinx
A Breakthrough in Insider Threat Detection & Prevention

IBM Business Partner

Tivoli. Compliance Insight Manager

© 2009 IBM Corporation

Payment Card Industry Compliance– How System z can help



*It is the customer's responsibility to identify, interpret and comply with any laws or regulatory requirements that affect its business. IBM does not represent that its products or services will ensure that the customer is in compliance with the law.

© 2009 IBM Corporation

Example: System z Solution Edition for Security PoV

How

Client Scenario: Mid-sized Retailer, Bullet-proof Mainframe security, hundreds of stores

- Store uses WEP wireless for Point of Sale devices and common password
- Point-of-Sale devices process credit and debit card transactions directly with banks
- Store managers run inventory transactions to mainframe; no encryption on sign-in

IBM Sales Team targets the CIO and CFO:

"Based on our expertise, we know that the weakest security link in an enterprise is typically the end user interface. It is through these interfaces that Hackers access your critical data, often without detection".

"Your current in-store network and interfaces are soft-targets for Hackers, exposing your firm to millions in losses"

Provocation:

"At this very moment, Hackers may be intercepting your clients POS card transactions and your first indication of a problem may come by way of a class action lawsuit. Also, your Store Managers may be unwittingly providing Hackers easy access to your Corporate data, stored on the Mainframe. IBM can secure your Enterprise if action is taken NOW.

IBM

Global Services:
Security & Privacy Consulting

zAAP
zIIP

Point of Sale

z/OS PKI Services

VENAFI

Intellinx
A Breakthrough in Insider Threat Detection & Prevention

IBM Business Partner

Tivoli. Compliance Insight Manager

Solution Edition for Security

Mainframe Security Extended end-to-end across the Enterprise

© 2009 IBM Corporation

Example: Tivoli zSecure Point of View

How

Client Scenario: Regional Utility Company, budget pressures, solid Mainframe security

- Highly instrumented electrical grid with multiple distribution points
- Automated service management for critical sensors and generators
- Mainframe security solid but not extended to devices and access points

IBM Sales Team targets the CIO and CFO:

"Of all the critical components in any Country's infrastructure, the power grid is one of the most vulnerable to cyber attack. With the permission of Utility Companies, Security Experts were able to hack into electric, water, and refinery grids"

"Your Company is exposed to attack, which will lead to millions in lost revenue and destroyed capital equipment"

Provocation:

"At this very moment, Hackers may be accessing critical grid components, taking control of sensors and generators,, with the purpose of causing an electric grid failure and a catastrophic explosion. You are exposed to monetary losses, as well as, the real potential of loss of life. Moreover, such an outage could lead to overall system failure, affecting the country's National Security.

As Reported by "60 Minutes" News Program:
http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml?tag=contentMain;cbsCarousel

"We know that cyber intruders have probed our electrical grid, and that in other countries cyber attacks have plunged entire cities into darkness," said President Obama.

Mainframe Security Extended end-to-end across the Enterprise

© 2009 IBM Corporation

System z Solution Edition for Security – Fraud Reference Case

Client Scenario: State Criminal Justice System, Bullet-proof Mainframe security, Many access points

- Policemen access Driver information from portal within Police cruiser
- Detectives track case data via Cognos Analytics application
- Courts manage search warrants and court cases

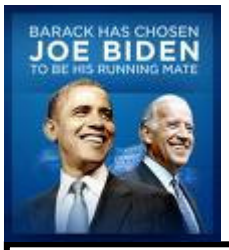
IBM Sales Team targets the CIO and CFO:

"Experience has demonstrated that insider leaks may be utilized to help criminals escape prosecution or to release information about celebrities or high ranking government officials".

"Your current IT infrastructure is exposed to these leaks which will likely result in civil and criminal penalties"

Provocation:

"At this very moment, policemen or detectives may be leaking information to criminals or the media. Also you are currently exposed to illegal access of sensitive information. Most alarming is that you may only become aware of such illegal access after your department has become fodder for the Tabloids. In such cases, departments have suffered high-level resignations and civil penalties



"Joe Biden selected as Obama's running mate"

Illegal queries

Wants and Warrants Database

Intellinx
A Breakthrough in Insider Threat Detection & Prevention

IBM Business Partner

zAAP zIIP

Tivoli. Compliance Insight Manager

Solution Edition for Security

Mainframe Security Extended end-to-end across the Enterprise

© 2009 IBM Corporation

System z Solution Edition for Security – Secure Infrastructure

Client Scenario: Large Healthcare Provider, Rigorous HIPAA compliance, huge patient records

- Secured access to patient medical records
- Patient records accessed by Doctors, Nurses, and Administration
- All Patient information is subject to HIPAA Compliance

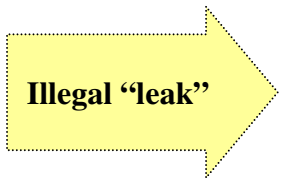
IBM Sales Team targets the CIO and CFO:

"Experience has demonstrated that insider leaks may be the biggest exposure to HIPAA compliance, especially when there is an opportunity to profit from disclosing patient records to third parties"

"Your current IT infrastructure is exposed to these leaks which will likely result in civil and criminal penalties"

Provocation:

"At this very moment, nurses, Doctors, or administrative personnel may be accessing patient records for the purpose of selling the information to a Tabloid. Such leaks are not only embarrassing and tarnish the Corporate image, they most certainly will result in substantial compliance and legal penalties, impacting the bottom-line. Failure to address this issue will expose you to negligence charges."



Intellinx
A Breakthrough in Insider Threat Detection & Prevention

IBM Business Partner

Tivoli. Compliance Insight Manager

Solution Edition for Security

Mainframe Security Extended end-to-end across the Enterprise

© 2009 IBM Corporation

Why monitoring the Criminal Justice Systems?

Scenario #1 – Information Leakage

- **Warrant information was disseminated to an unauthorized person. How do you find out who accessed it?**
- **A State Police employee leaks information on planned arrests in a homicide case investigation to one of the suspects. How can you stop it in time?**

Scenario #2 – Providing Evidence to Court

- **A request is received from a court to verify that a user did or did not use the system to perform his job duties. How can you provide the evidence?**

Scenario #3 – Investigation needs

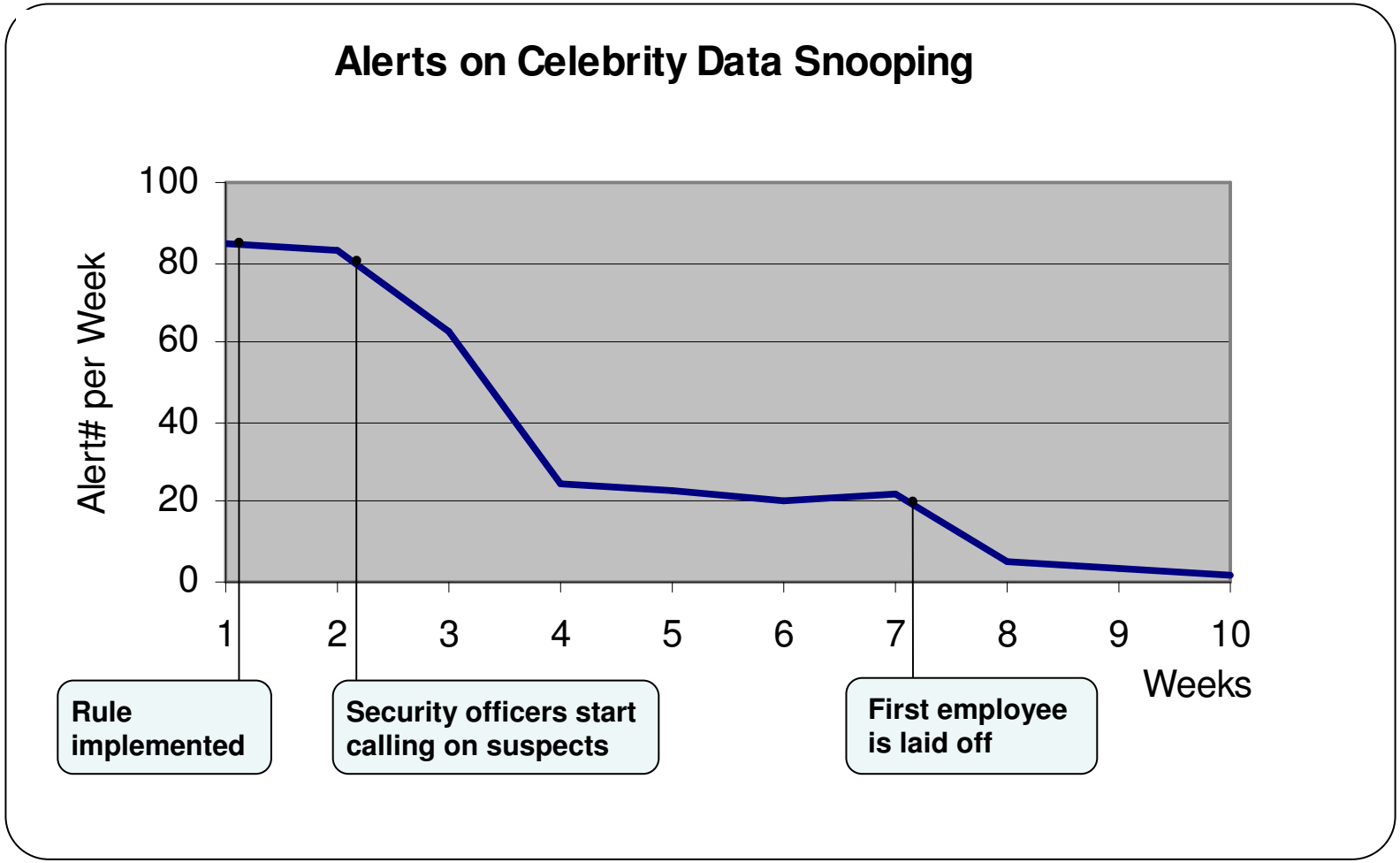
- **A vehicle with a certain tag may have been used in a homicide and law enforcement is searching to locate where vehicle was last seen. How do you find out?**

Scenario #4 – Privileged User planting a Logical Bomb

- **A disgruntled programmer plants malicious code which sporadically deletes customer accounts. How do you reveal what he did?**

© Intellinx Ltd. All Rights Reserved.Intellinx Ltd. All Rights Reserved
© 2009 IBM Corporation

The Deterrence Factor of Real-time Alerts



© Intellinx Ltd. All Rights Reserved.Intellinx Ltd. All Rights Reserved
© 2009 IBM Corporation

System z Solution Edition for Security – Encryption Reference Case

Client Scenario: Large Airline, Web enabled reservation system, High volume transaction processing

- Consumers and Travel Agents leverage SOA portal to access reservations
- 10,000's of tickets sold daily via the web
- Secure access for client access and privacy is essential to workflow

IBM Sales Team targets the CIO and CFO:

"Encryption is leveraged to protect personally identifiable information transmitted across the internet. Each application is signed to ensure that spoofing cannot occur. Self signed certificates are used by application developers to speed deployment. However, transactions fail when certificates expires".

"Your system is not immune to this issue and when certificates expire, your online reservations will fail"

Provocation:

"You currently lack a central control point to manage certificate expiration. Failure to detect an impending expiration will lead to an outage that will result in lost bookings. Based on your transaction volumes, your firm will lose $3M dollars per day in perishable reservations. This need not be left to chance….IBM has a solution to eliminate this costly exposure"

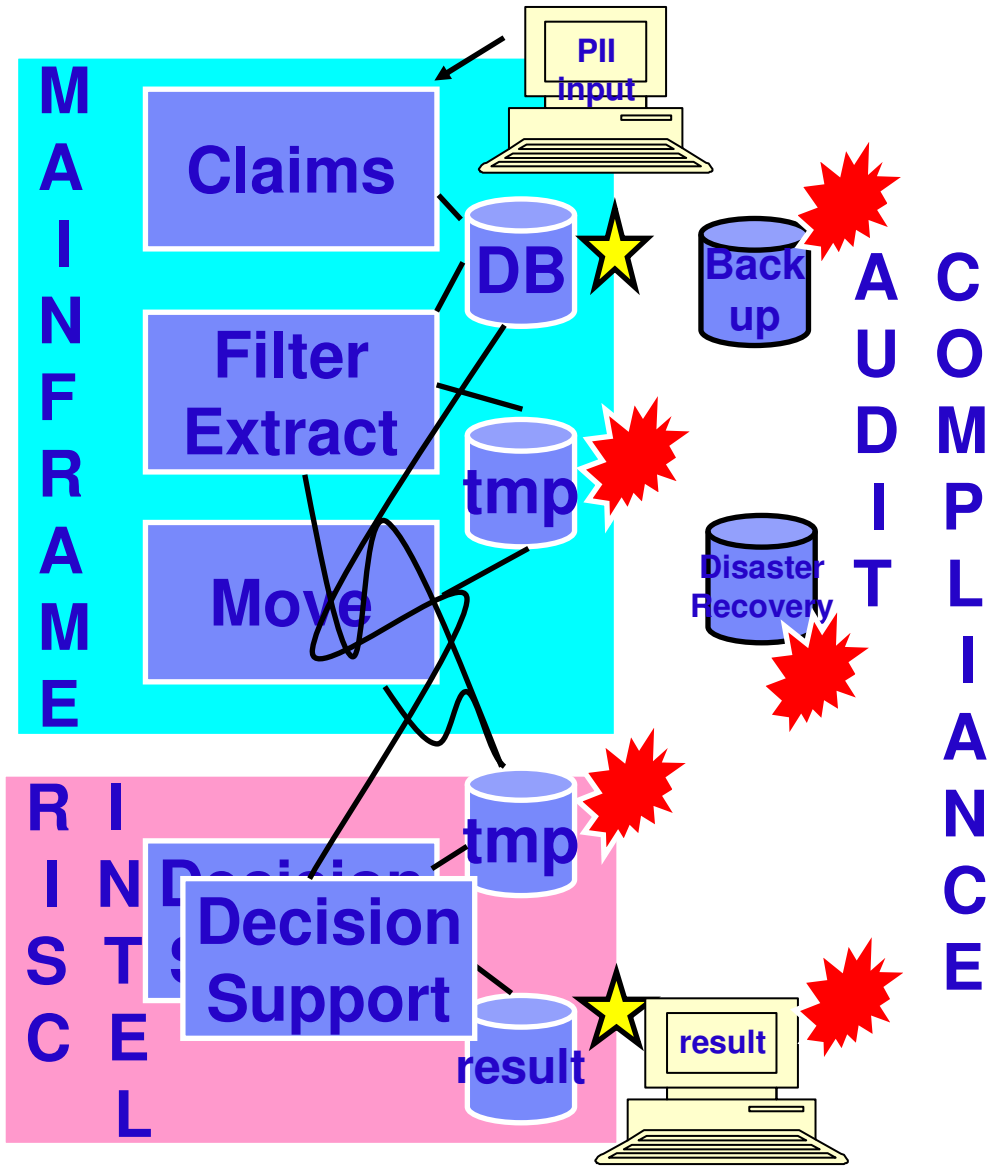
= **Lost Revenues (and Customers)**

Solution Edition for Security

Mainframe Security Extended end-to-end across the Enterprise

© 2009 IBM Corporation

Why does Infrastructure simplification matter? HIPAA, Sarbanes-Oxley



Typical Business Workflow

- **Do you audit all places with Personally Identifiable Information?**
  - Is the process automated?
- **Data is easy to replicate**
- **Policies are not.**
  - Reducing the copies will reduce compliance efforts and increase resiliency
    - Leverage a file server to delete copies and reduce data movement
    - Application data proximity
      - Move the applications back to the data source, where practical
      - Plus, able to use WebSphere SOA access facilities, where practical

System z: The Data Vault

© 2009 IBM Corporation

System z Solution Edition for Security – CI&AM Reference Case

Client Scenario: Automobile manufacturer, automated assembly line, employee administration

- Many applications across a wide variety of systems
- Critical workflows to ensure automated assembly line
- 10,000 active employees that communicate with critical applications

IBM Sales Team targets the CIO and CFO:

"Common roles defined across workflow processes are critical to business success. Registration and enrollment of users must be rapid and consistent across application environments ".

"300,000 former employees, who have retired or terminated, still have discrete ids and access to critical data."

Provocation:

"Your firm is susceptible to espionage and/or sabotage from former employees. You are putting your operations at risk because of the ad hoc provisioning of users to disparate systems. Failure to centralize the administration and removal of unauthorized people from your systems (in a timely fashion) could cost you millions. IBM can help you eliminate this risk and potential for future loss"

In the News: Former **DuPont** employee used access to steal trade secrets on OLED.

In the News: Disgruntled employee of International **Financial Services organization** planted "logic bomb" which deleted 10 billion files and affected over 1300 servers causing **$3M in losses.**

Tivoli. Compliance Insight Manager

Intellinx

A Breakthrough in Insider Threat Detection & Prevention

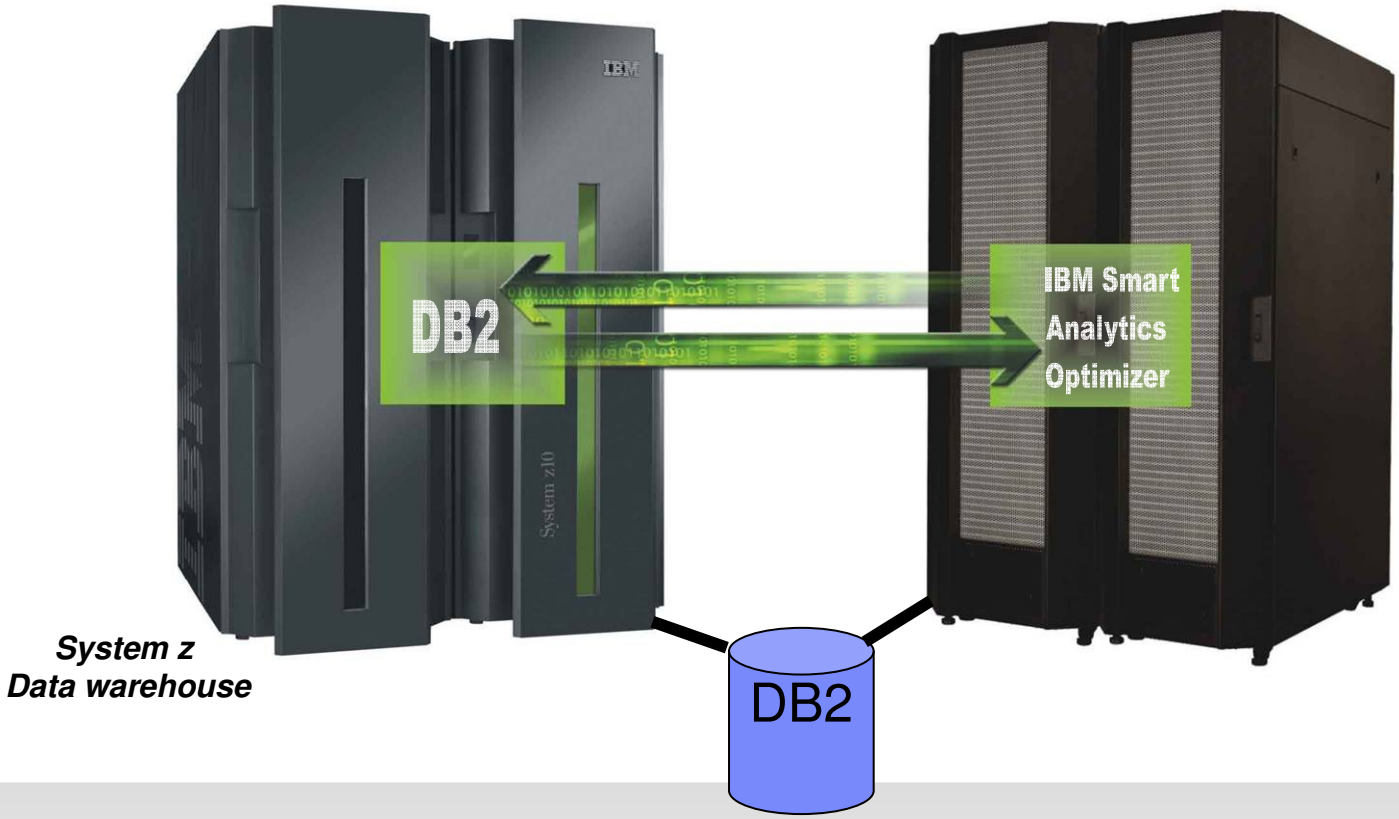
IBM Business Partner

Solution Edition for Security

Mainframe Security Extended end-to-end across the Enterprise

© 2009 IBM Corporation

An example of workload-optimized systems:
Introducing the IBM Smart Analytics Optimizer.



For an integrated business intelligence solution,

The future is here today.

© 2009 IBM Corporation

z/OS PKI Services is . . . Providing Trusted Identity

- A base element of z/OS V1R3 and higher
- It provides full certificate life cycle management
  - User request driven via customizable Web pages
  - Browser or server certificates
  - Automatic or administrator approval process
  - Administered using the same Web interface
  - End user/administrator revocation process
  - Deploys CRL (Certificate Revocation List) and OCSP (Online Certificate Status Protocol)
  - Provides e-mail notification for completed certificate request and expiration warnings

BANCO DO BRASIL

- **30 million accounts**
- **4,000 locations**
- **20 million transactions per day**

- Avoids an estimated $16 million a year in digital certificate costs
- Establishes a more secure enterprise network
  - **by becoming their own Certificate Authority instead of paying third party**

© 2009 IBM Corporation

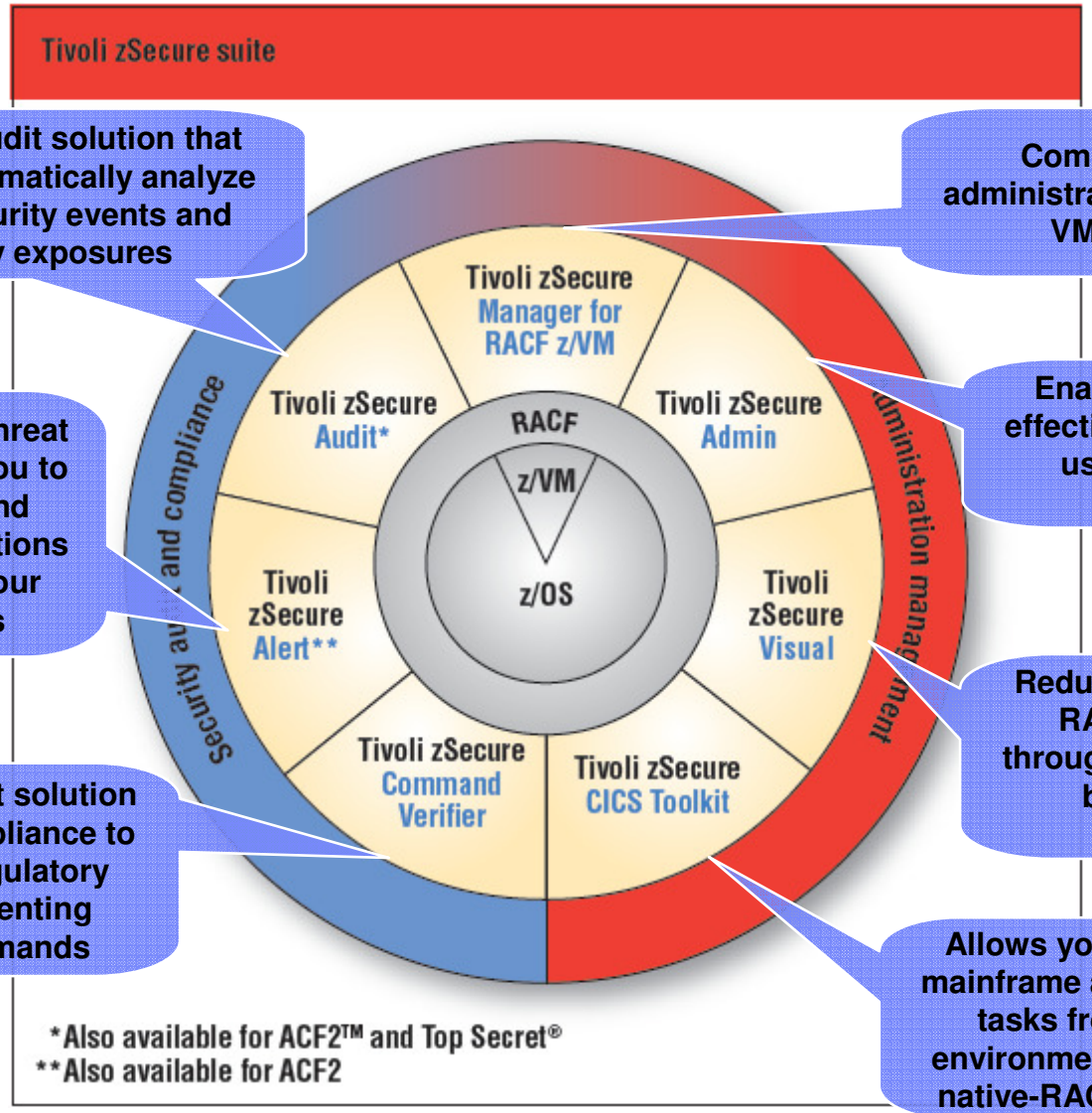
Solution Edition for Security: Highlights

- 5 security solutions that contain hardware, software, and services
  - **Each includes a recommended comprehensive list of non-integrated Security products**
    - **You choose what you need!**
  - **Each is available on one of the following: z10 EC, z10 BC, z9 EC, z9 BC, or an LPAR on an existing z9® or z10 System z ® processor**
  - **Each includes 400 hours of services for implementation / configuration**
  - **Each sold at highly discounted prices!**

- **Enterprise Fraud Analysis**
  - **Record and playback insider actions, forensic analysis to discover relationships, real-time prevention workflow applied to operations**
- **Enterprise Encryption and Key Management**
  - **Protecting personally identifiable data; enterprise encryption: Discover, audit and monitor and serve encryption keys**
- **Centralized Identity & Access Management**
  - **Cross platform user provisioning and management; cross platform authentication services**
- **Securing Virtualization: z/VM®, Linux for System z**
  - **Easily secure new virtualized workloads; security lifecycle management of server images running in Linux for System z, improved readiness for private cloud**
- **Compliance / Risk Mitigation / Secure Infrastructure: z/OS®**
  - **Audit and Alert processing, Simplified management operations, Data anonymization for development and test**

© 2009 IBM Corporation

IBM Tivoli zSecure Suite



Compliance and audit solution that enables you to automatically analyze and report on security events and detect security exposures

Combined audit and administration for RACF in the VM environment

Real-time mainframe threat monitoring allowing you to monitor intruders and identify mis-configurations that could hamper your compliance efforts

Enables more efficient and effective RACF administration, using significantly less resources

Reduces the need for scarce, RACF-trained expertise through a Microsoft Windows–based GUI for RACF administration

Policy enforcement solution that enforces compliance to company and regulatory policies by preventing erroneous commands

Allows you to perform mainframe administrative tasks from a CICS environment, freeing up native-RACF resources

Note: ACF2 and Top Secret are either registered trademarks or trademarks of CA, Inc. or one of its subsidiaries.

© 2009 IBM Corporation

DB2, IMS and IBM Data Encryption on System z

Protecting sensitive and confidential data

Database Capabilities

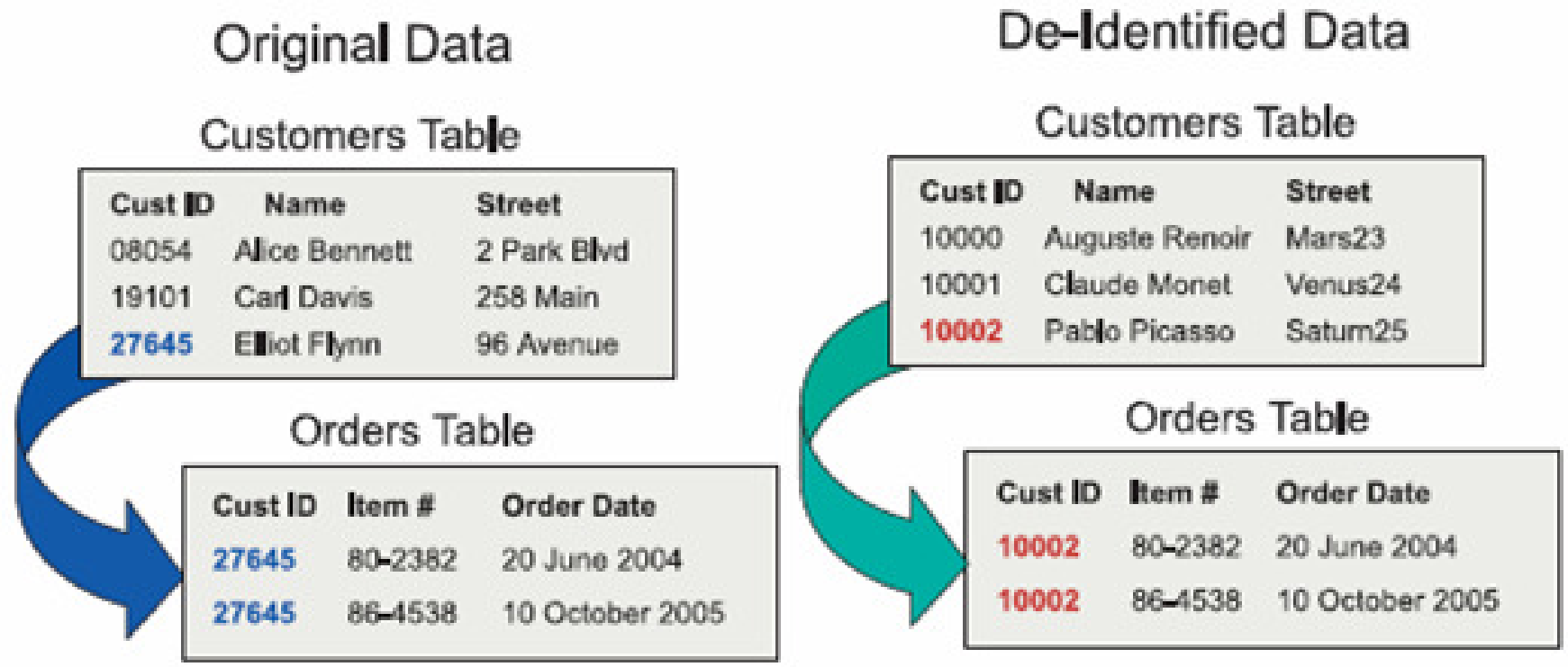
- Provides access control to DB2/IMS resources via DB2/IMS / RACF Interface including:
  - Resource (plan/package/table) authorization
  - Role based security (with DB2 v9, IMS v9/10 and RACF 1.8)
    - Network Trusted Context
    - Database Roles
  - MLS - Row Level Security (with DB2 v8, IMS v9/10 and RACF 1.7)
- Provides encryption support via SQL in V8
- Provides trace facility performance and functionality improvements

Encryption Capabilities

- Provides a single tool for encrypting both IMS and DB2 data
- Can be customized at the IMS segment level and at the row level for DB2
- Uses hardware encryption for the fastest possible encryption
- Runs as an EDITPROC
- Supports either clear key or secure key
- Exploits zSeries and S/390 Crypto Hardware features, which results in low overhead encryption/decryption
- Data is protected using encryption algorithms approved by the U.S. National Institute of Science and Technology

© 2009 IBM Corporation

Optim Test Data Generation – leverage this to build test versions of Analytic DB's for Operational Risk



Optim offers a variety of data masking techniques to protect the confidentiality of private information.

© 2009 IBM Corporation

Mainframe as a Security Hub

- **z/OS is known for running mission-critical workloads for your Enterprise**
- **Ensuring your applications run and run securely is a business requirement**
- **z/OS offers highly available, secure, and scalable database hosting**
- **z/OS has well-honed security processing with very granular permissions capabilities**
- **z/OS offers superb auditing of operations performed**
- **control of user/group definitions in multiple registries, including RACF, from z/OS, is now available**
- **services-based security capabilities, hosted on z/OS and Linux for System z, are now available**
- **Using a combination of Linux for System z and z/OS systems, the mainframe can host the security functions for the Enterprise**

© 2009 IBM Corporation

© 2009 IBM Corporation