



# *Virtualization and Consolidation Options*

*What makes z simple and  
better*

*Jim Porell*

*IBM Distinguished Engineer*

*IBM System z Business Development*

*The future runs on System z*



# Agenda for Today

- **Virtualization**

- X86 on a mainframe?
  - What if?

- **Security**

- Why encryption matters
  - Role of Venafi with IBM
- Fraud, forensics, Real time prevention
  - Role of Intellinx with IBM

# 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.

# 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

# 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



*STRAIGHT DOPE ON THE VULNERABILITY DU JOUR FROM* **IBM Internet Security Systems**

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\*

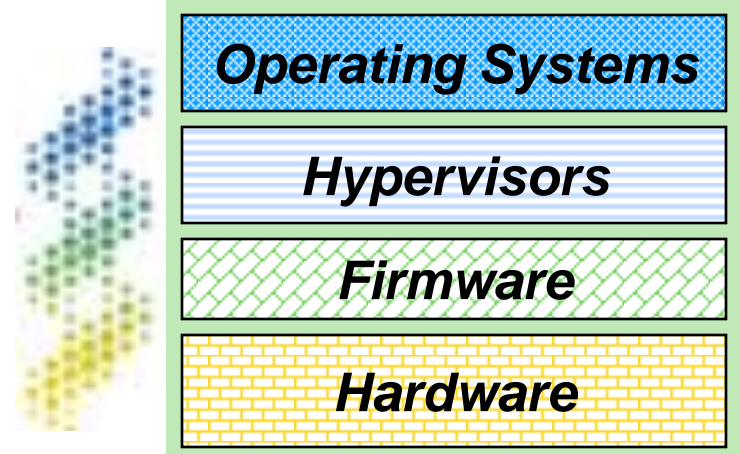
VMware Vulns by Year	Total Vulns	High Risk Vulns	Remote Vulns	Vulns in 1 <sup>st</sup> Party Code	Vulns in 3 <sup>rd</sup> Party Code
Vulns in 2003	9	5	5	5	4
Vulns in 2004	4	2	0	2	2
Vulns in 2005	10	5	5	4	6
Vulns in 2006	38	13	27	10	28
Vulns in 2007	34	18	19	22	12

## Virtualization & Security Topics

<b>Adding Virtualization to:</b>		<b>Virtualization Attributes:</b>
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
<b>Competitive posture</b>		

# IBM System z Virtualization Genetics

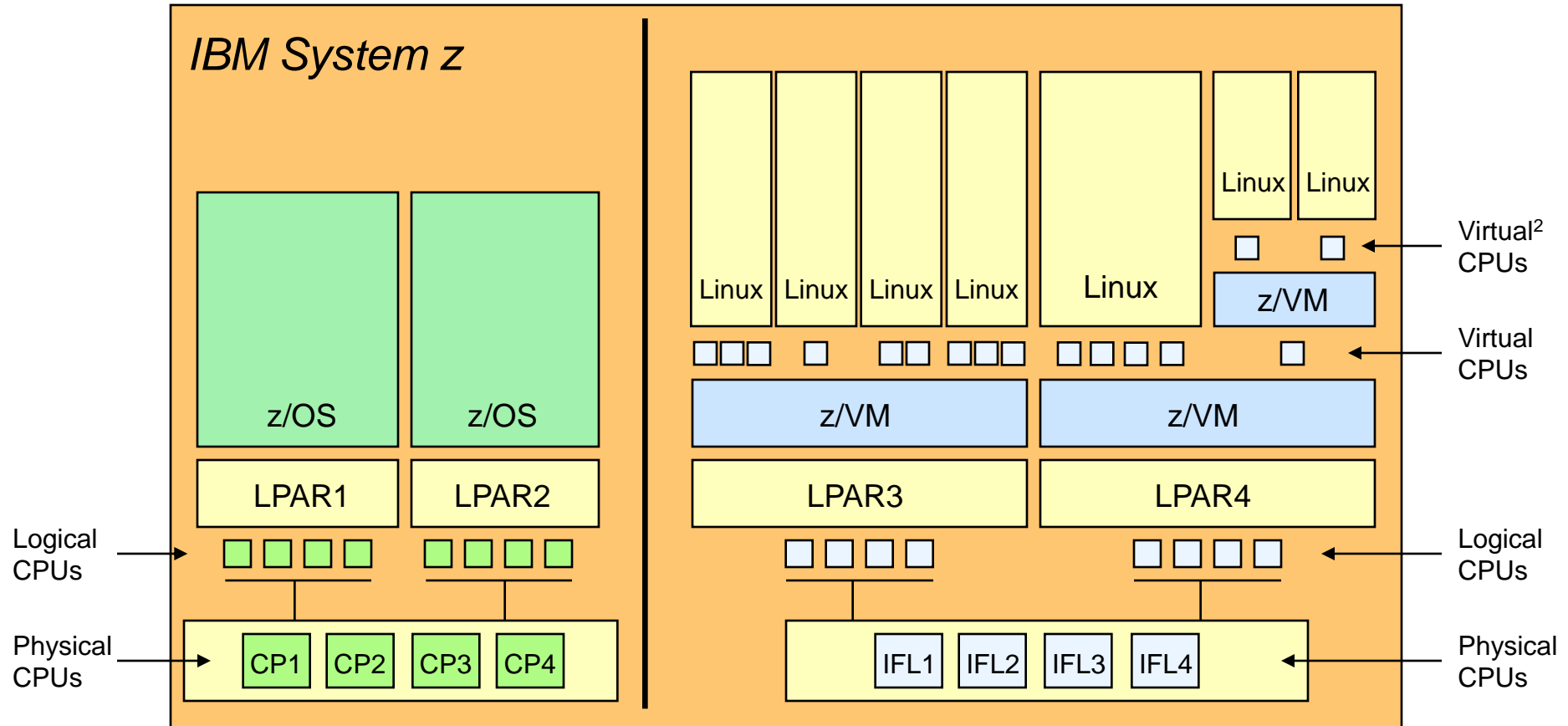
- System z is ***thoroughly*** architected to host applications in a virtualized environment
- This is accomplished with a coordinated set of investments that permeate the technology stack of ***hardware***, ***firmware***, ***hypervisors***, and ***operating systems***
- This means clients can maximize 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



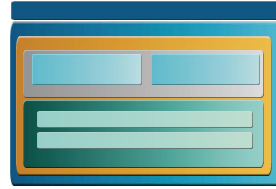


# IBM System z Virtualization Leadership

## Extreme Levels of CPU Sharing

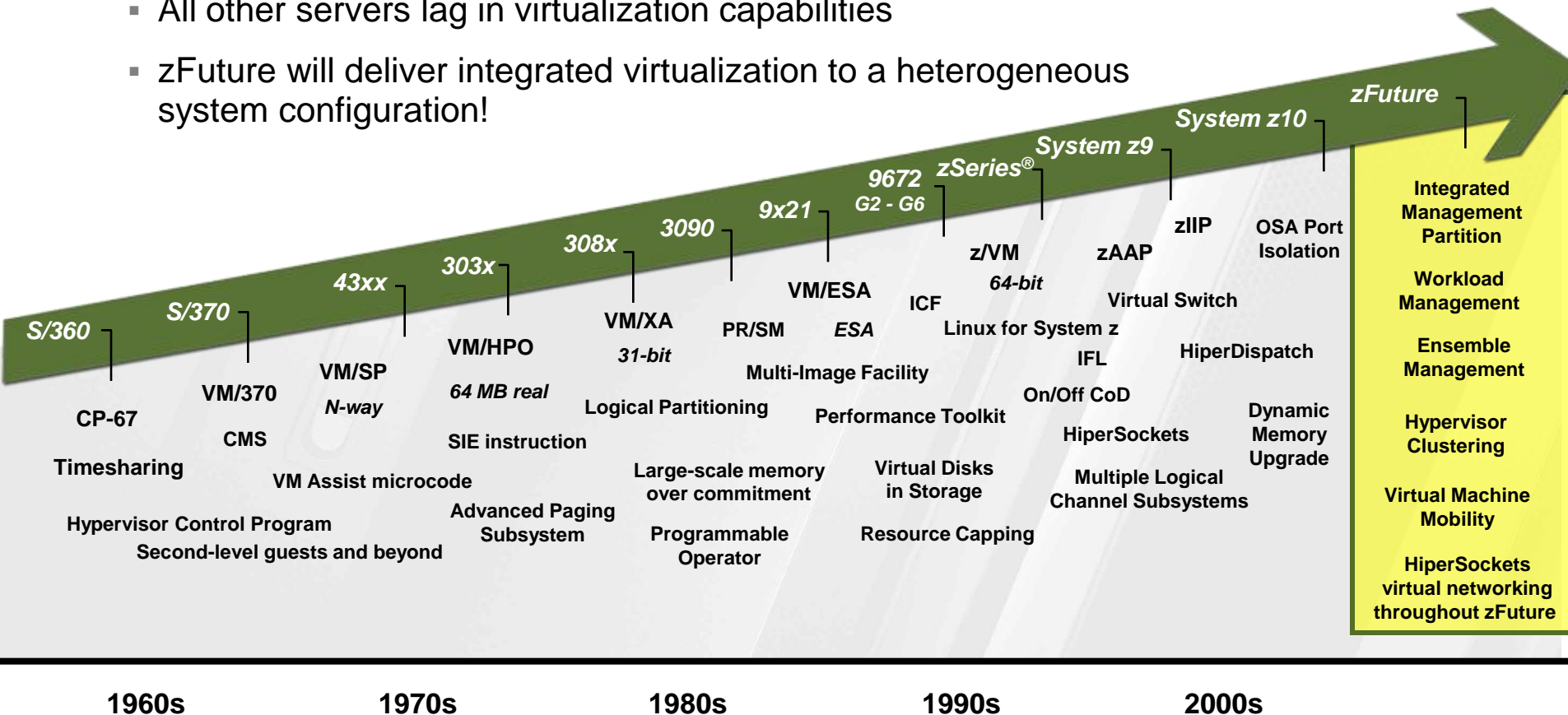






# zFuture: The next leap in virtualization

- 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!



# Tooling

## Assemble Solution

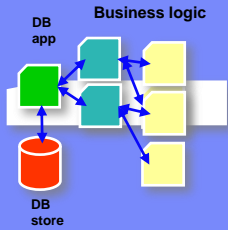


Image Library

# 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

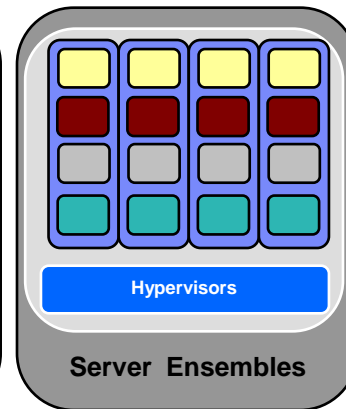
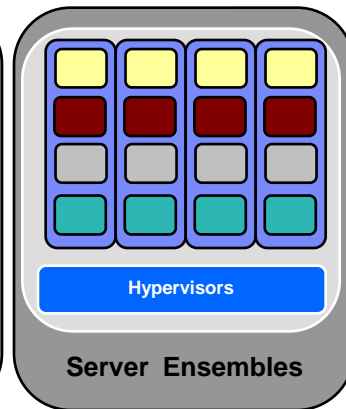
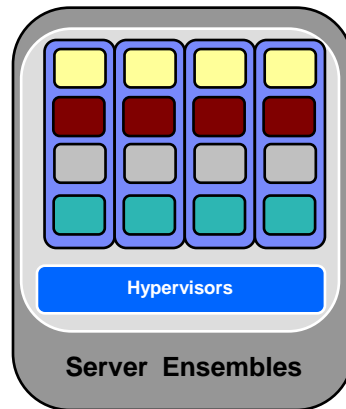
### Ensemble Management Interfaces

## Ensemble Management

### System z Ensemble

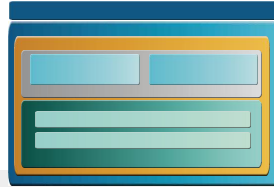
### Power Systems® Ensemble

### 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



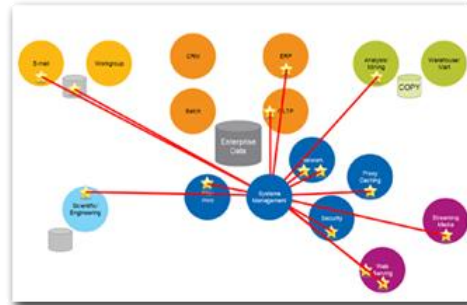
# System z ensemble

## System z Future

### System z Mainframe



### Integrated Systems Management firmware

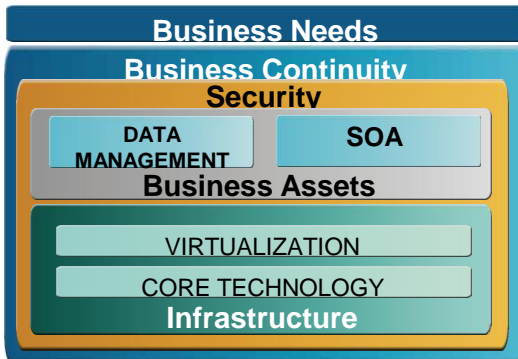


### Accelerators

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

### Application Serving Blades

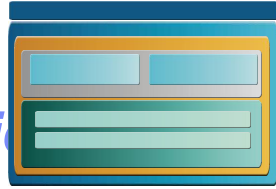
- Logical device integration between System z resources and application serving commodity devices
- Providing competitive price-performance and improved QoS for applications with a close affinity to mainframe data



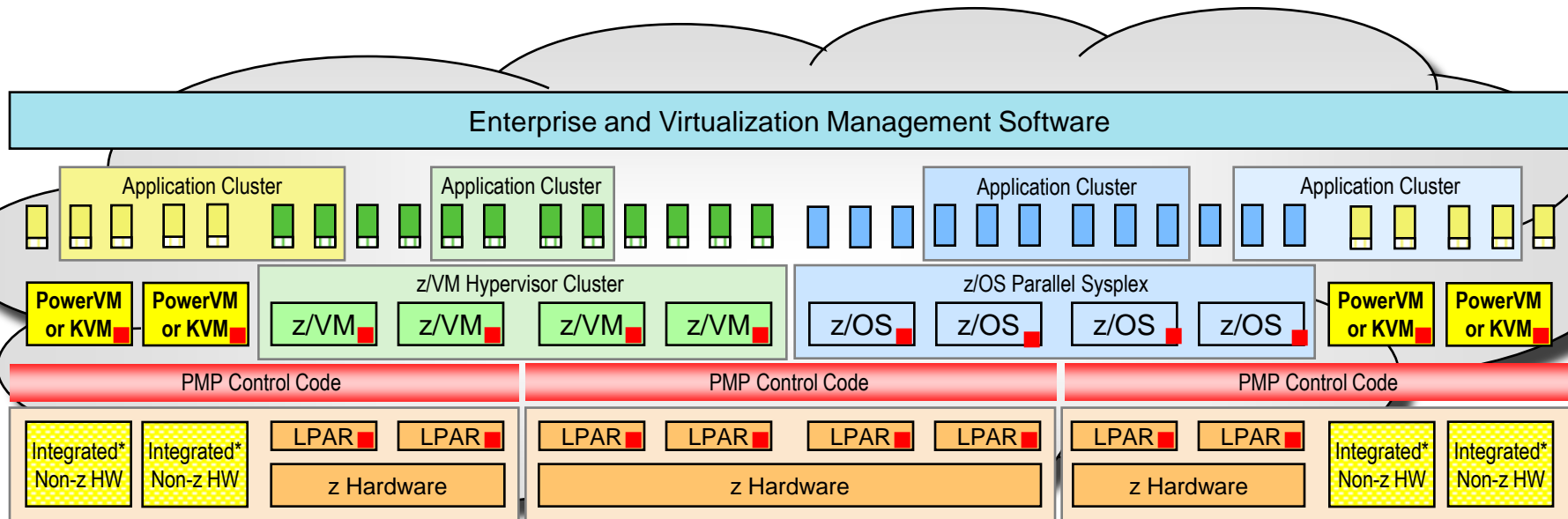
- Integrate, monitor, and manage multi-OS resources as a single, logical virtualized system
- Single WLM, Security, and System Management interface across all resources

# IBM multi-architecture virtualization – Conceptual view

## *System z multi-system, federated Hypervisor configuration*



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

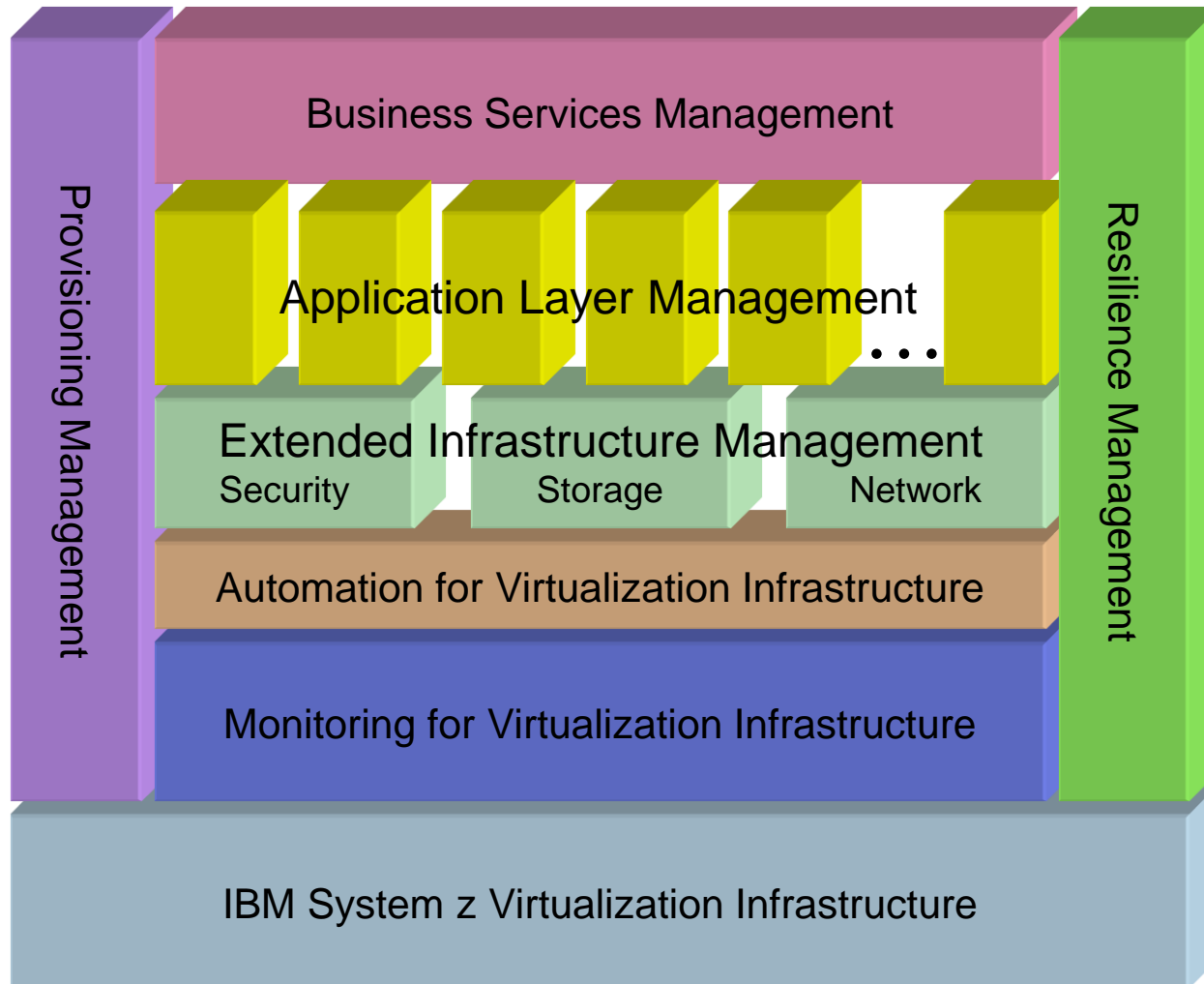


■ = Code that interfaces with Platform Management Partition (PMP)

\* E.g., Cell Broadband Engine, DataPower, Power Blades, x86\_64

# IBM Tivoli Virtualization Management for System z

## *Helping Clients Manage and Control Their Virtualized IT Infrastructure*



# 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

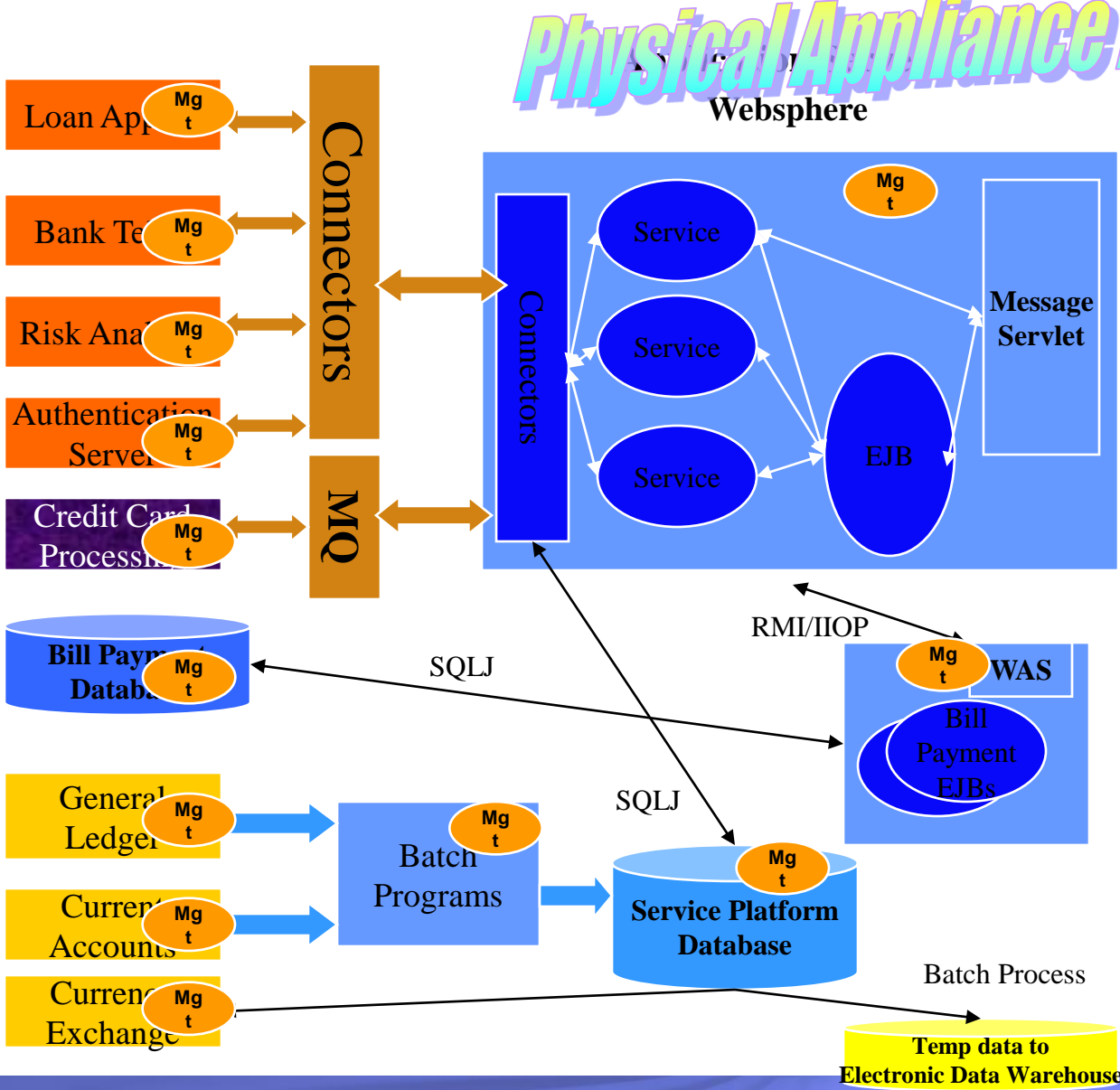
Helps secure your virtual servers and reduce business risk

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

Increase staff productivity and virtualize the enterprise

# Typical multi-system Design: Numerous Mgmt Domains

## Physical Appliance Model

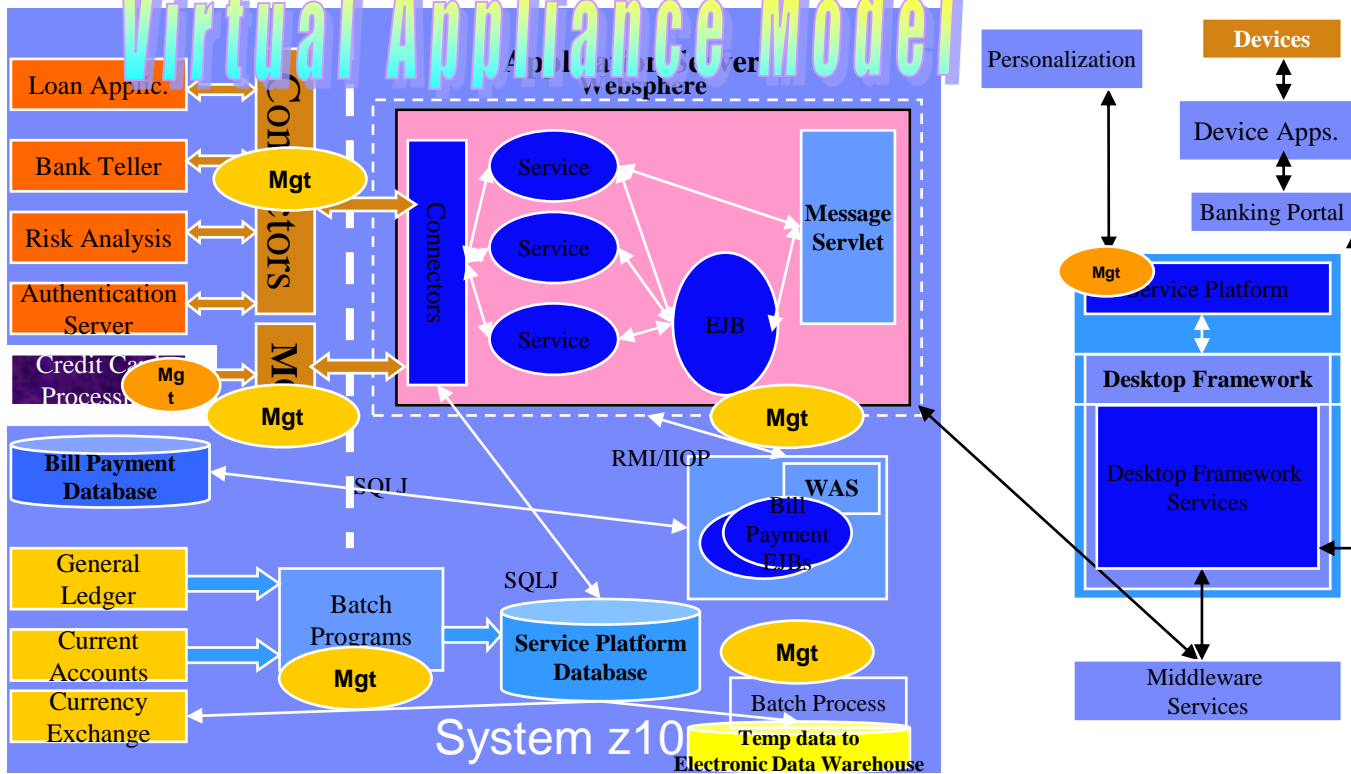


Mgt

- 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



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



## Potential advantages of consolidating your application and data serving

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

With IFL

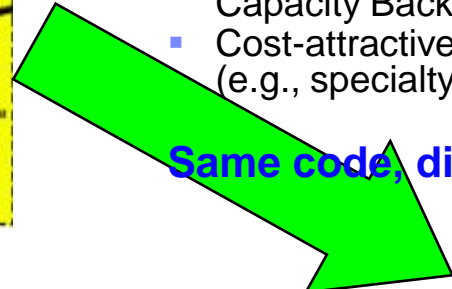
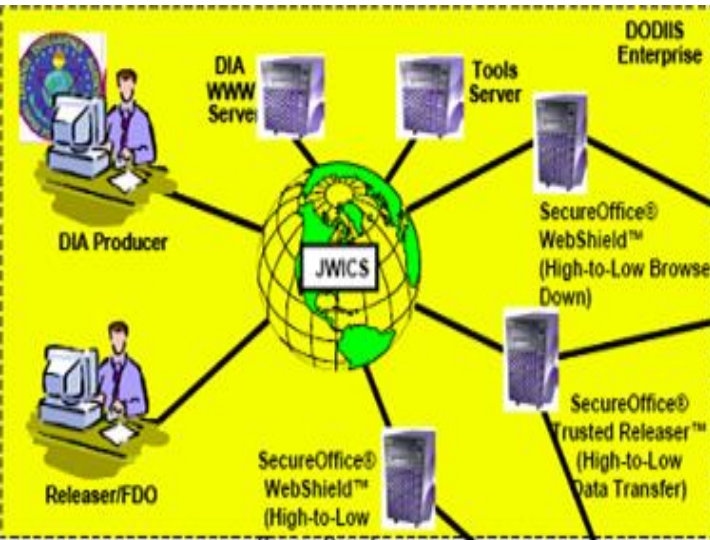
With zAAP  
& zIIP



# Secure Virtualization Changes Operational Model

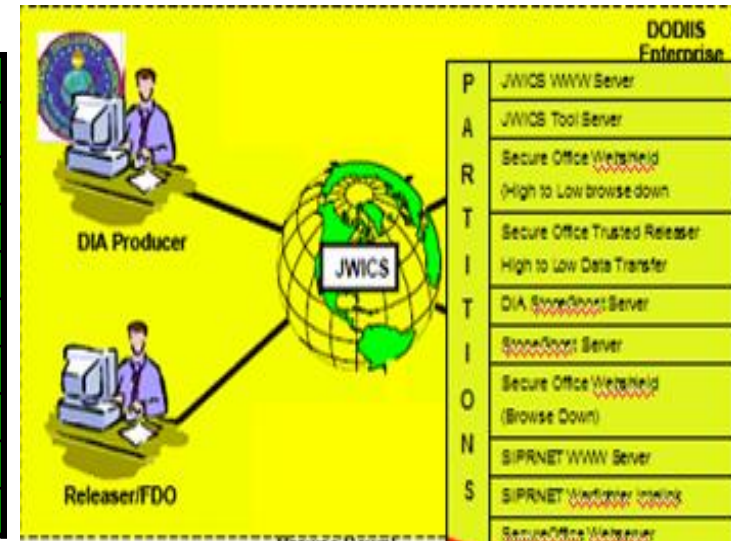
## Opportunities for Cost Savings

- 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)

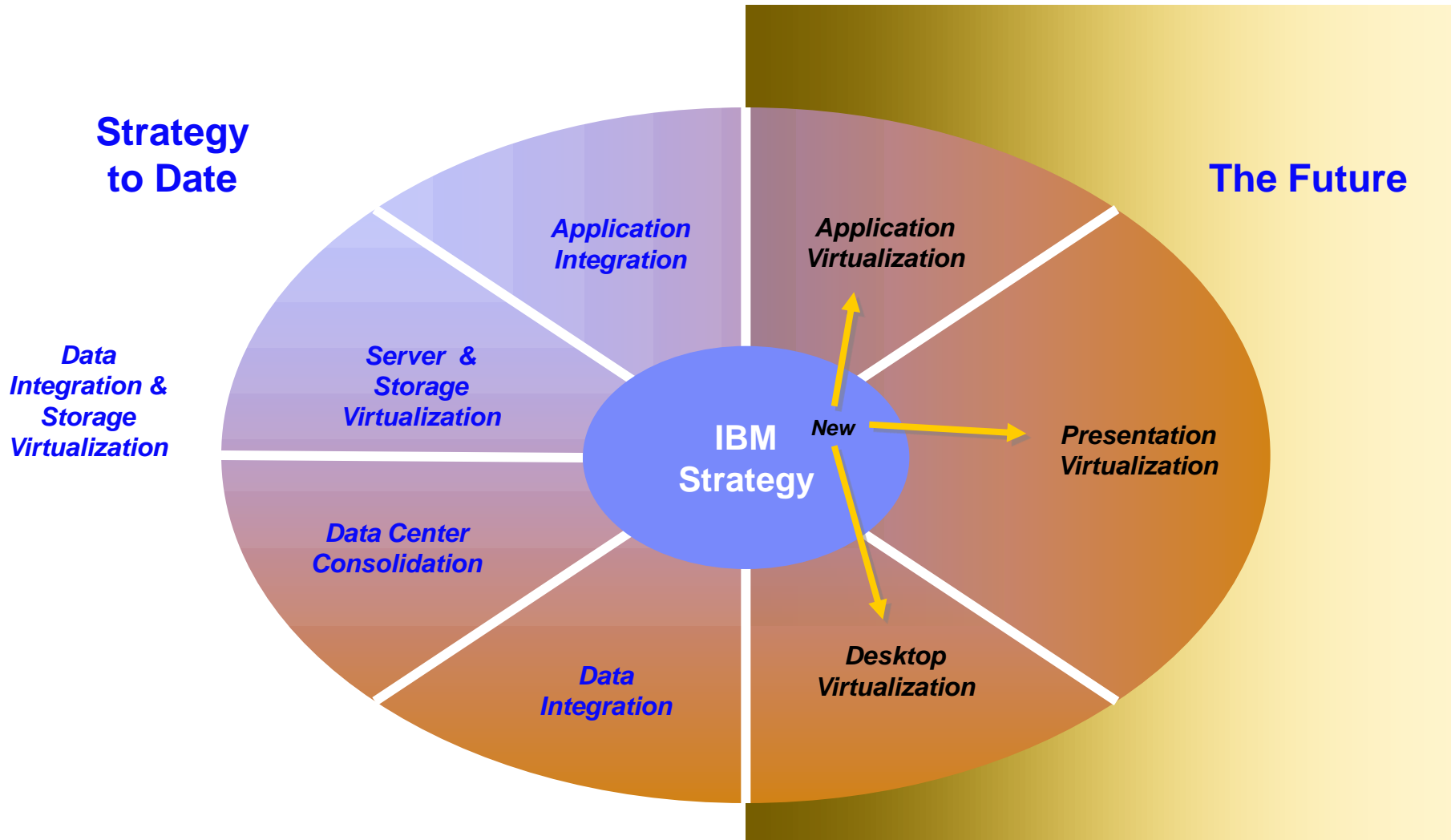


Same code, different container, superior operations!

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

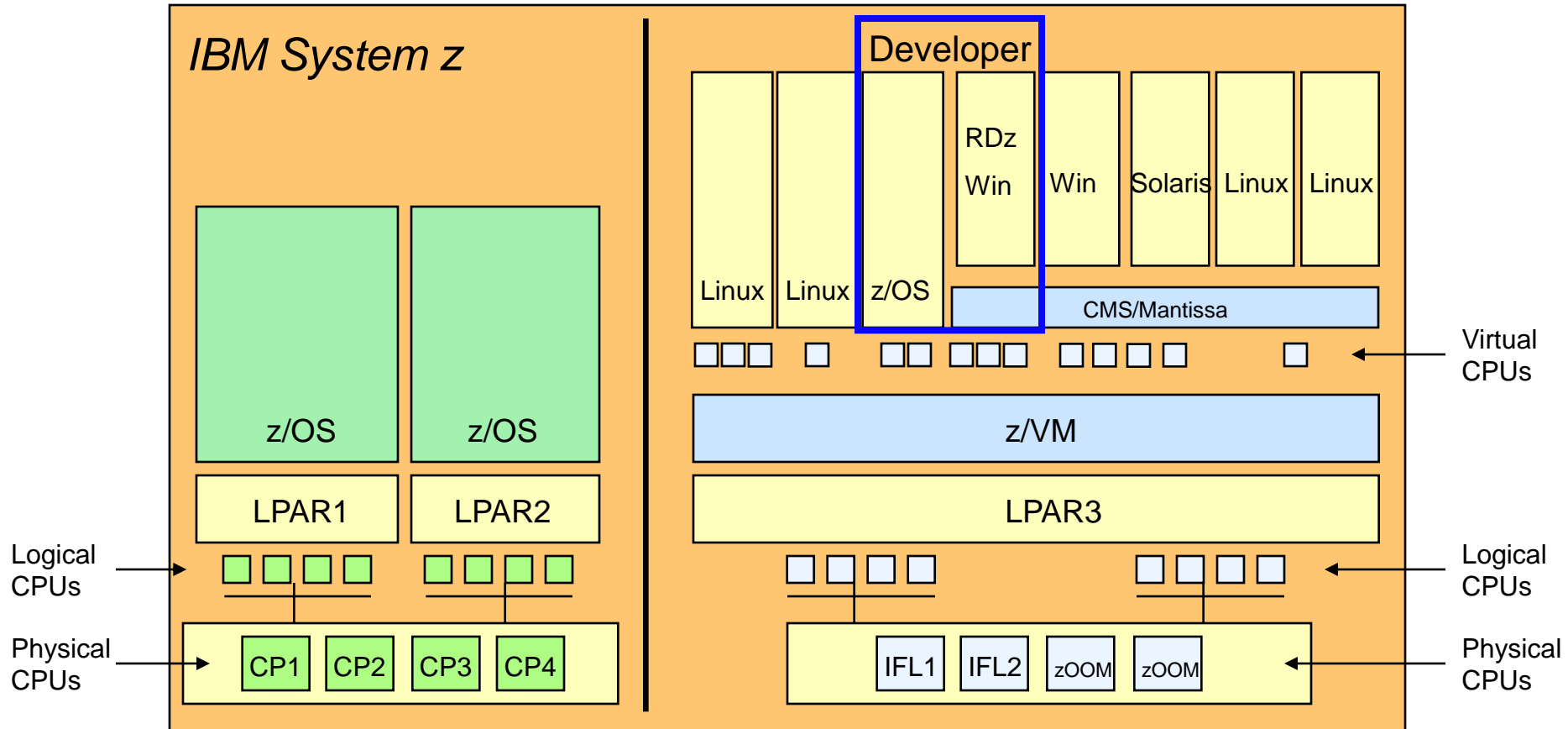


Our premise: The market is at a tipping point – with the right investment in client consolidation and virtualization, IBM can re-shape the way our customers define their security strategy (and subsequent spend)



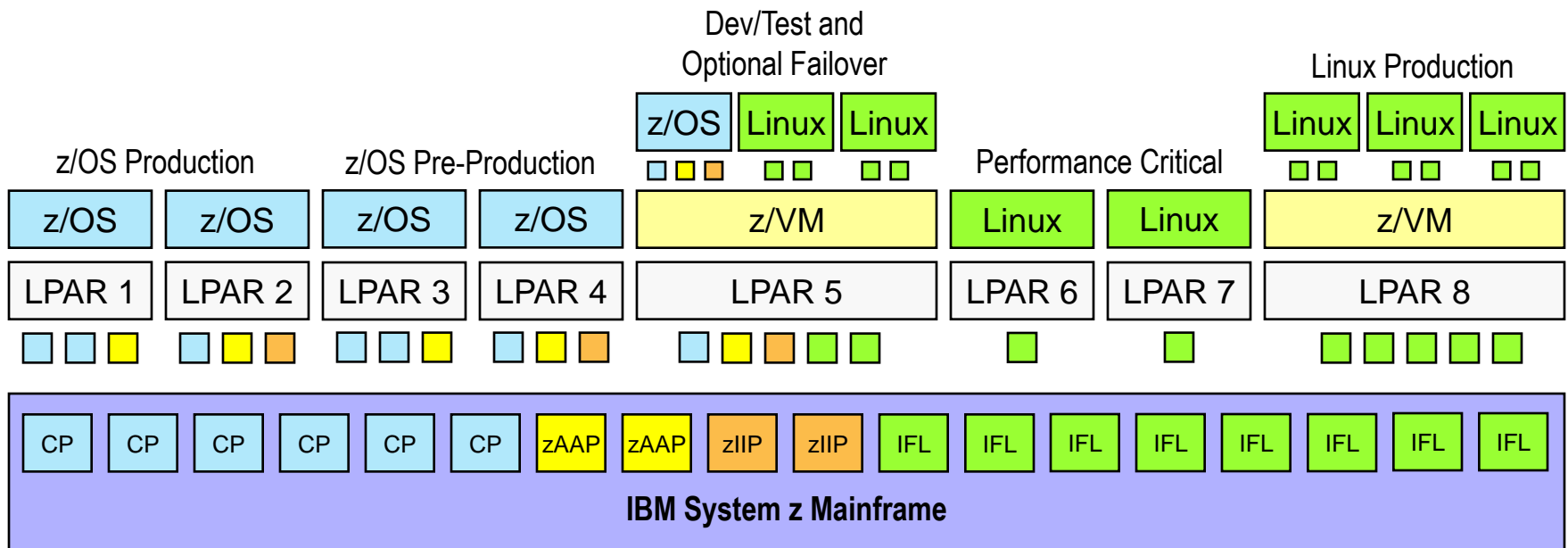
# IBM System z Virtualization Leadership

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



# 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)



# 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                 |

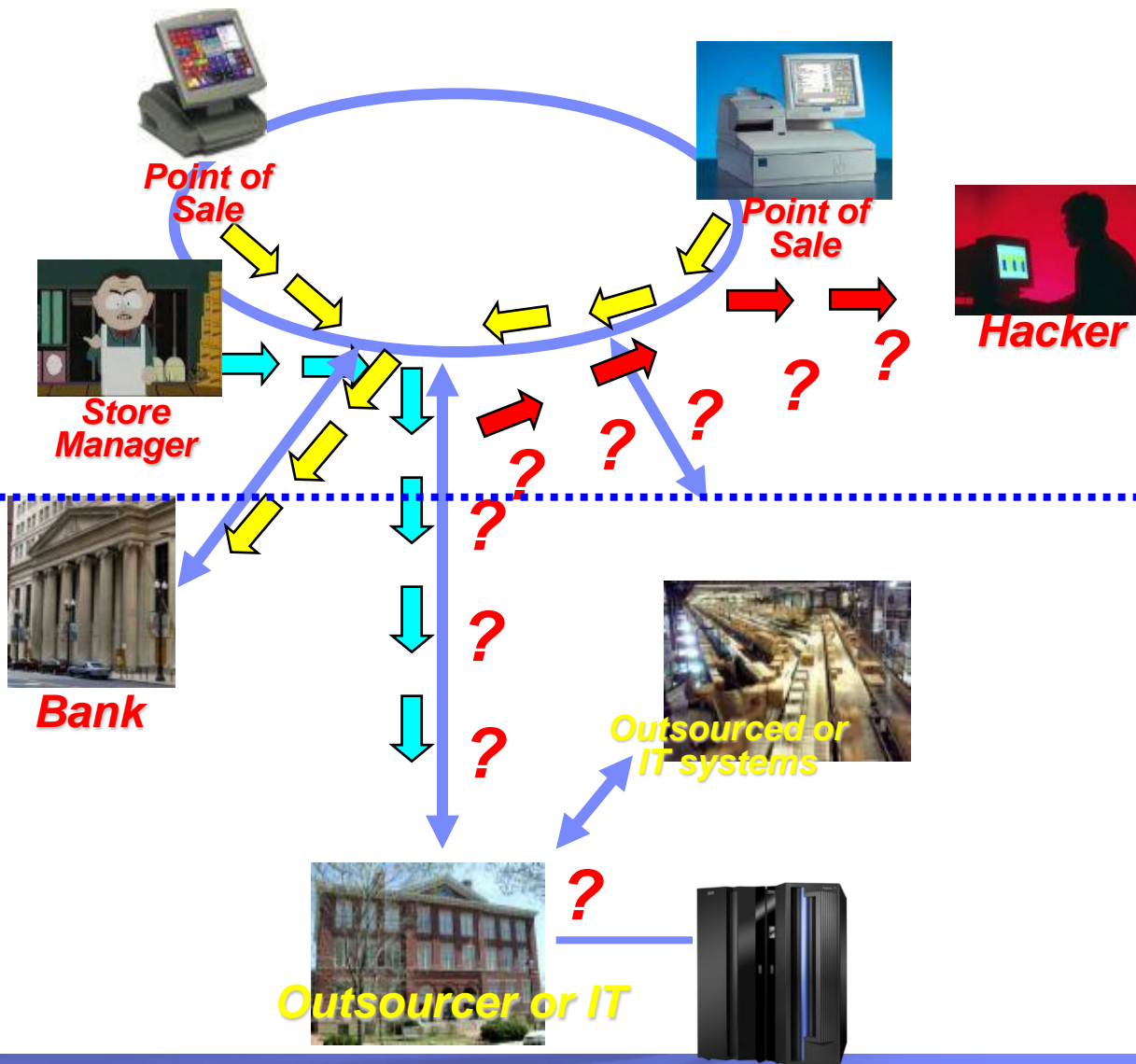
## Regularly Monitor and Test Networks

- |     |   |
|-----|---|
| 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 |
|-----|--|

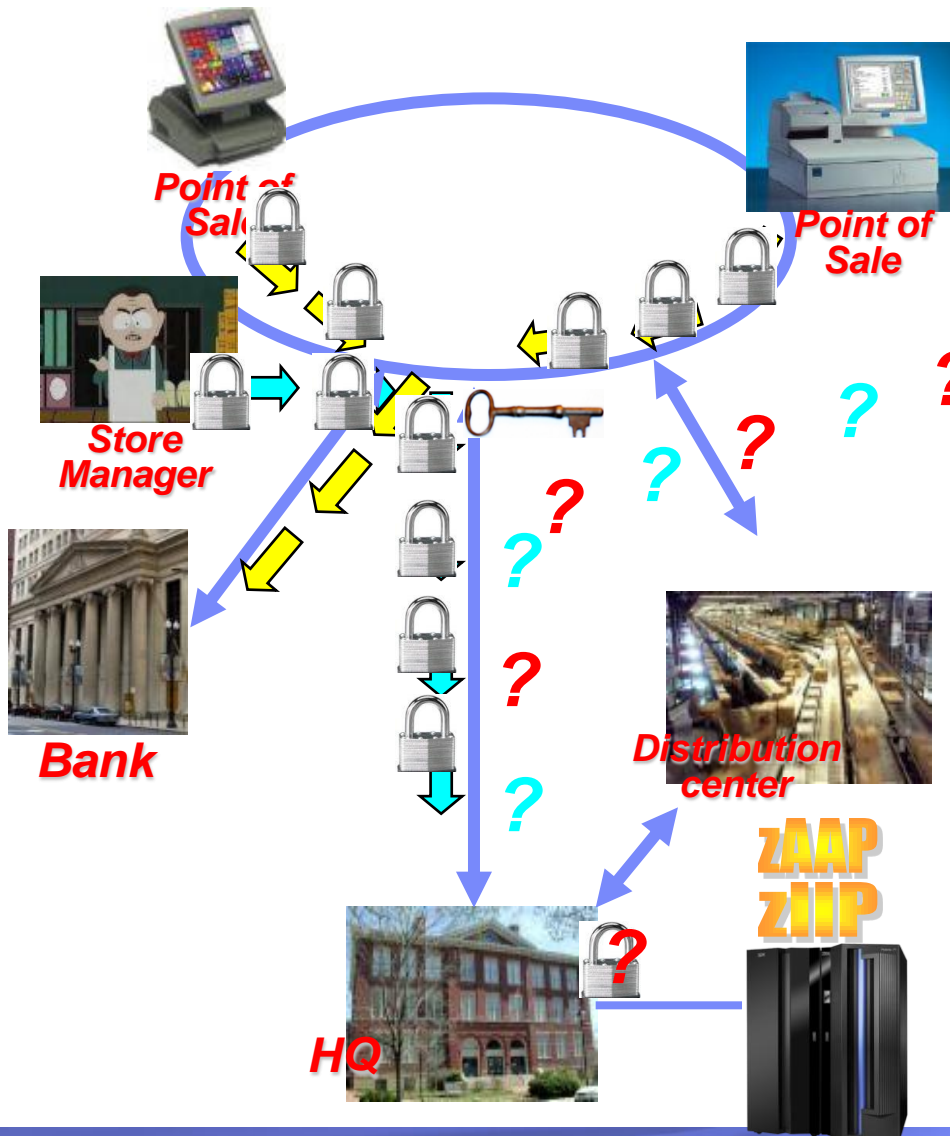
# Real Customer Problem



- 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
- Hypothesis: Mainframe could help secure stores if they use good procedures
- Store managers run inventory transactions to mainframe
- No encryption on sign in
- No audit records analyzed



# 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



Global Services:  
Security & Privacy  
Consulting

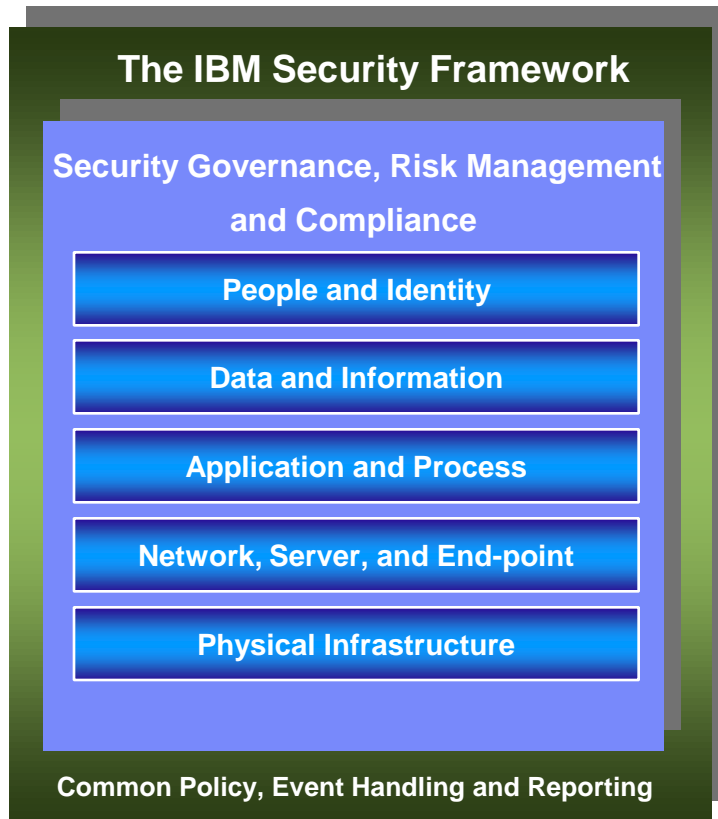


A Breakthrough in Insider Threat Detection & Prevention



**Tivoli Compliance Insight Manager**

# IBM Security Framework



## ■ IBM delivers:

- Timely **visibility** into business continuity risks and compliance posture
- More effective **control** over utilization of sensitive business assets
- Efficient **automation** of the identification and remediation of vulnerabilities and the addressing of compliance mandates

## IBM Security Solutions



### • SECURITY COMPLIANCE

- Demonstrable policy enforcement aligned to regulations, standards, laws, agreements (PCI, FISMA, etc..)



### • IDENTITY & ACCESS

- Enable secure collaboration with internal and external users with controlled and secure access to information, applications and assets



### • DATA SECURITY

- Protect and secure your data and information assets



### • APPLICATION SECURITY

- Continuously manage, monitor and audit application security



### • INFRASTRUCTURE SECURITY

- Comprehensive threat and vulnerability management across networks, servers and end-points



# IBM's History in Security Technology

- **IBM Common Cryptographic Architecture CCA**
- **Lucifer II (Feistel 1975) and Data Encryption Standard DES (1977)**
- **IBM Resource Access Control Facility RACF (1976)**
- **Quantum Cryptography (Bennett, Brassard 1984)**
- **Elliptic Curve Cryptography ECC (Koblitz, Miller, 1985)**
- **Citadel Secure Crypto Coprocessor (1992)**
- **Random Oracle Model of Cryptography (Bellare, Rogaway, 1993)**
- **Keyed-Hash Message Authentication Code HMAC (Bellare, Canetti, Krawczyk, 1996); went into RFC 2104, FIPS PUB 198, and is standard in TLS and IPsec**
- **Cramer-Shoup Encryption (first provably secure and practical public key encryption system; Cramer/Shoup, 1998)**
- **Digital Immune System (w/ Symantec, 1999)**
- **Cancelable Biometrics (Ratha, Connell, Bolle, 2001)**
- ***Acquisition of Access360 (2002)***
- **Hippocratic Database (Agrawal, Kiernan, Srikant, Xu, 2002)**
- **Web Services Security Architecture, with Microsoft (2002)**
- **Anonymous Entity Resolution (Jeff Jonas (SRD), 2003)**
- **OASIS eXtensible Access Control Markup Language (XACML) (Kudo for IBM + other companies, 2003)**
- **Direct Anonymous Attestation (w/ HP and Intel; Brickell, Camenisch, Chen, 2004)**
- **First Common Criteria certification of Linux, with Novell/Suse (2005)**
- ***Acquisition of Datapower (2005)***
- ***Acquisition of SRD (2005)***
- ***Acquisition of Micromuse / Netcool (2006)***
- ***Acquisition of Internet Security Systems (2006)***
- **First encrypted tape drive TS1120 (2007)**
- ***Acquisition of Princeton Softech (2007)***
- ***Acquisition of Consul Risk Management (2007)***
- ***Acquisition of Watchfire (2007)***
- ***Acquisition of Encentuate (2008)***

# Payment Card Industry Compliance— How System z can help

**Build & Maintain a Secure Network**

System z integrity features  
z/OS Network Policy Agent  
z/OS Intrusion Detection Services  
Linux on z as a DMZ

**Protect Cardholder Data**

Encryption Infrastructure  
Database Encryption & Test Tools  
Network encryption:  
SSL/TLS, IPsec, OpenSSH  
Tape encryption

**Maintain Vulnerability Mgmt Program**

z/OS Network Policy Agent  
z/OS Intrusion Detection Services  
IBM Internet Security Solutions

System z integrity features  
RACF and MLS  
Tivoli zSecure  
Tivoli Identity Manager

**Implement Strong Control Measures**

z/OS Healthchecker  
Tivoli zSecure  
Tivoli Compliance Insight Manager

IBM Services:  
Penetration Testing

**Monitor & Test Networks**

z/OS Network Policy Agent  
EAL & FIPS Certifications

IBM Services:  
Internet Security Solutions  
Security & Privacy Consulting

**Maintain Information Security Policy**

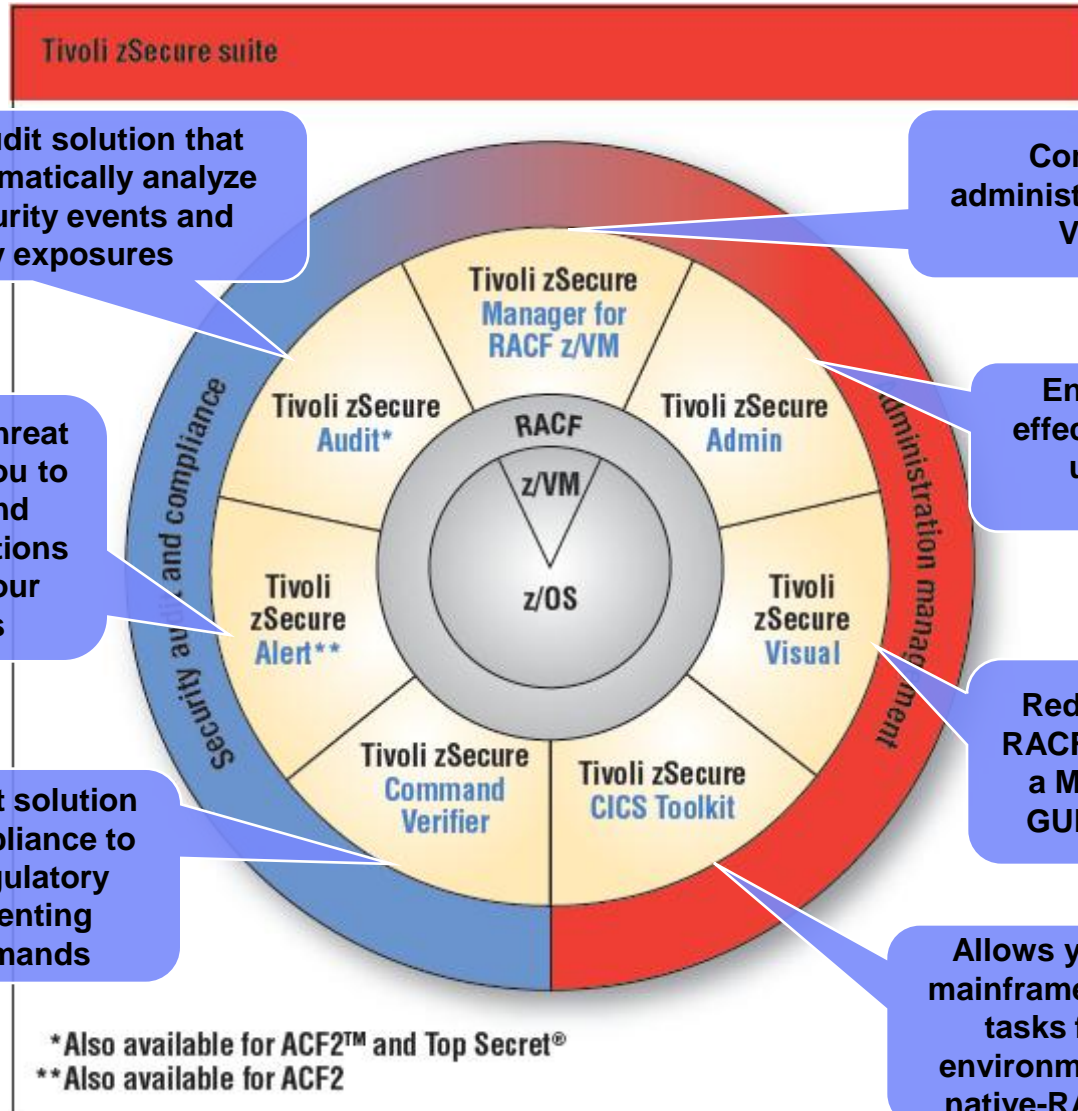
## z/OS PKI Services is . . .

- 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



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

# 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

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

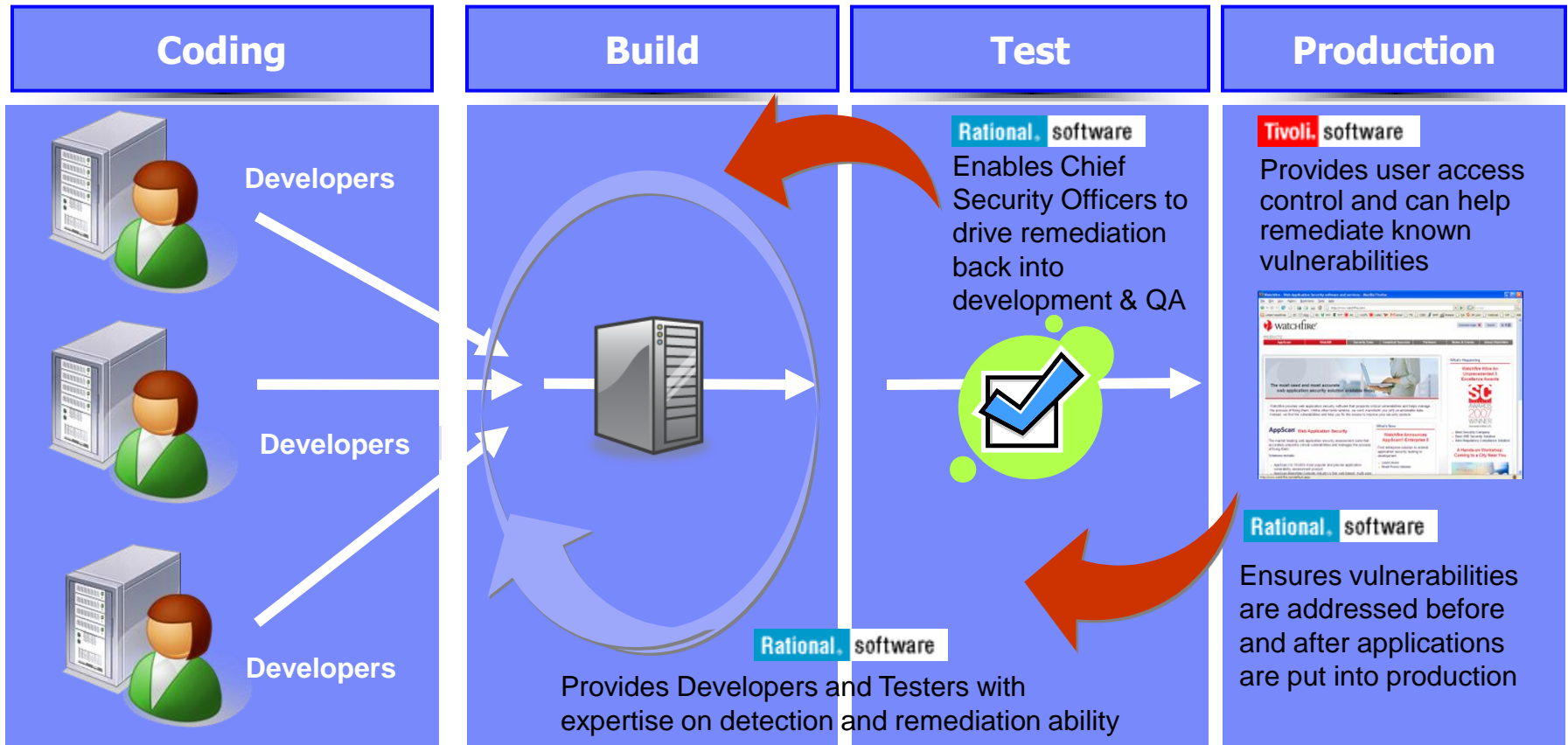
Reduces the need for scarce, RACF-trained expertise through a Microsoft Windows-based GUI for RACF administration

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

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

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

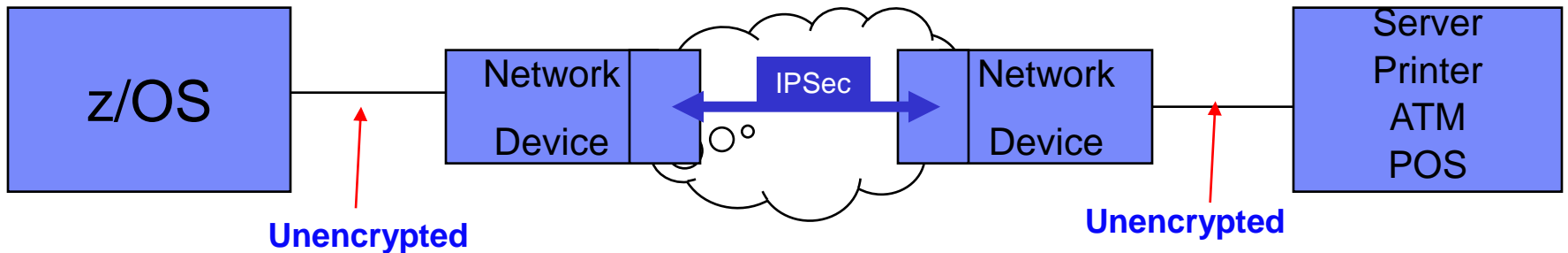
# Rational AppScan & IBM Tivoli provide security that spans the application lifecycle



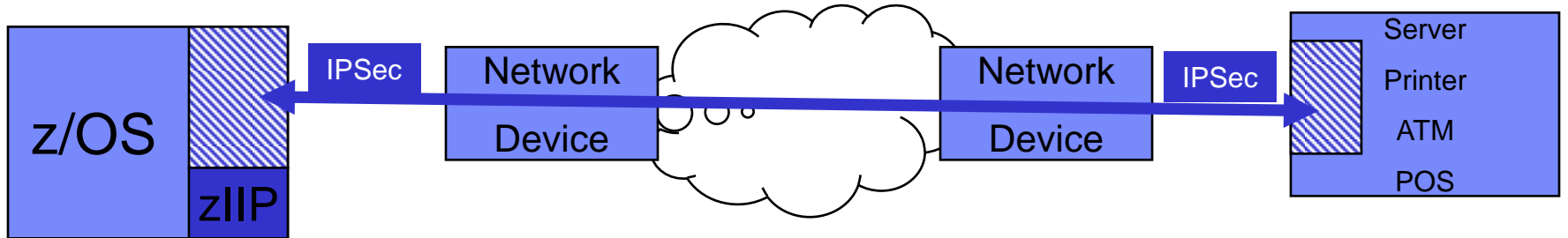
AppScan tests the application and RACF/Tivoli Access Manager secures access to them

# End-to-end network encryption

Growing requirement for companies that outsource some part of their network  
 zIIP specialty engine support helps reduce the cost of adding IPSec protection



**Encryption in network devices**



**End-to-end encryption**



# DB2, IMS and IBM Data Encryption on System z

*Protecting sensitive and confidential data*

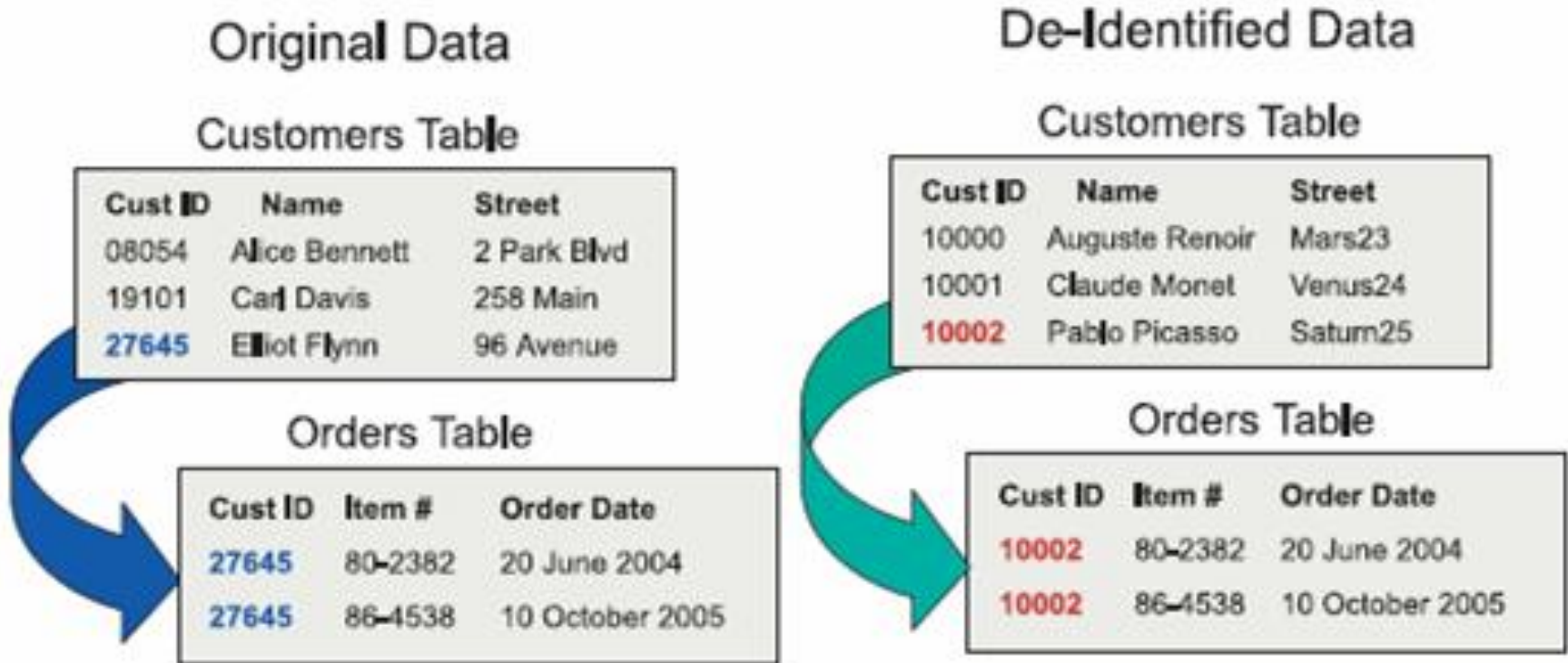
## Database Capabilities

- 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

# 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.*



# 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**



*The future runs on System z*

# Questions

