Virtualization and Consolidation Options

What makes z simple and better

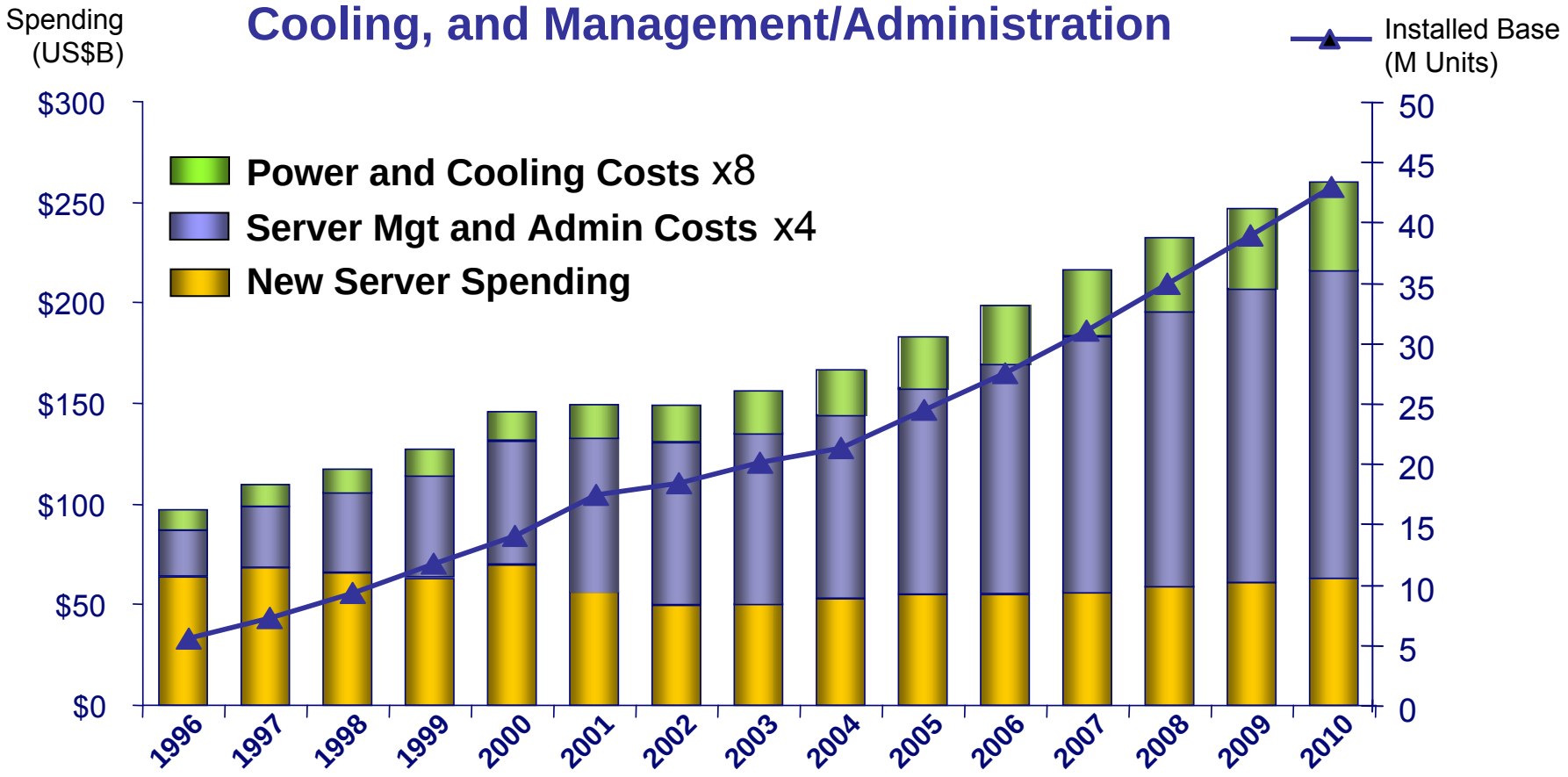
Jim Porell
IBM Distinguished Engineer
IBM System z Business Development

The future runs on System z

Topics

- **Business drivers for server consolidation**
- **System z: wired for virtualization**
- **System z workload management: what every business needs**
- **Save money, grow your business**

Worldwide IT Spending on Servers, Power and Cooling, and Management/Administration



Many servers, much capacity, low utilization = $140B unutilized server assets

Source: IDC, 2006

As server volumes increase, so does complexity, making basic business requirements like availability, security, and disaster recovery more difficult to achieve.

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.

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

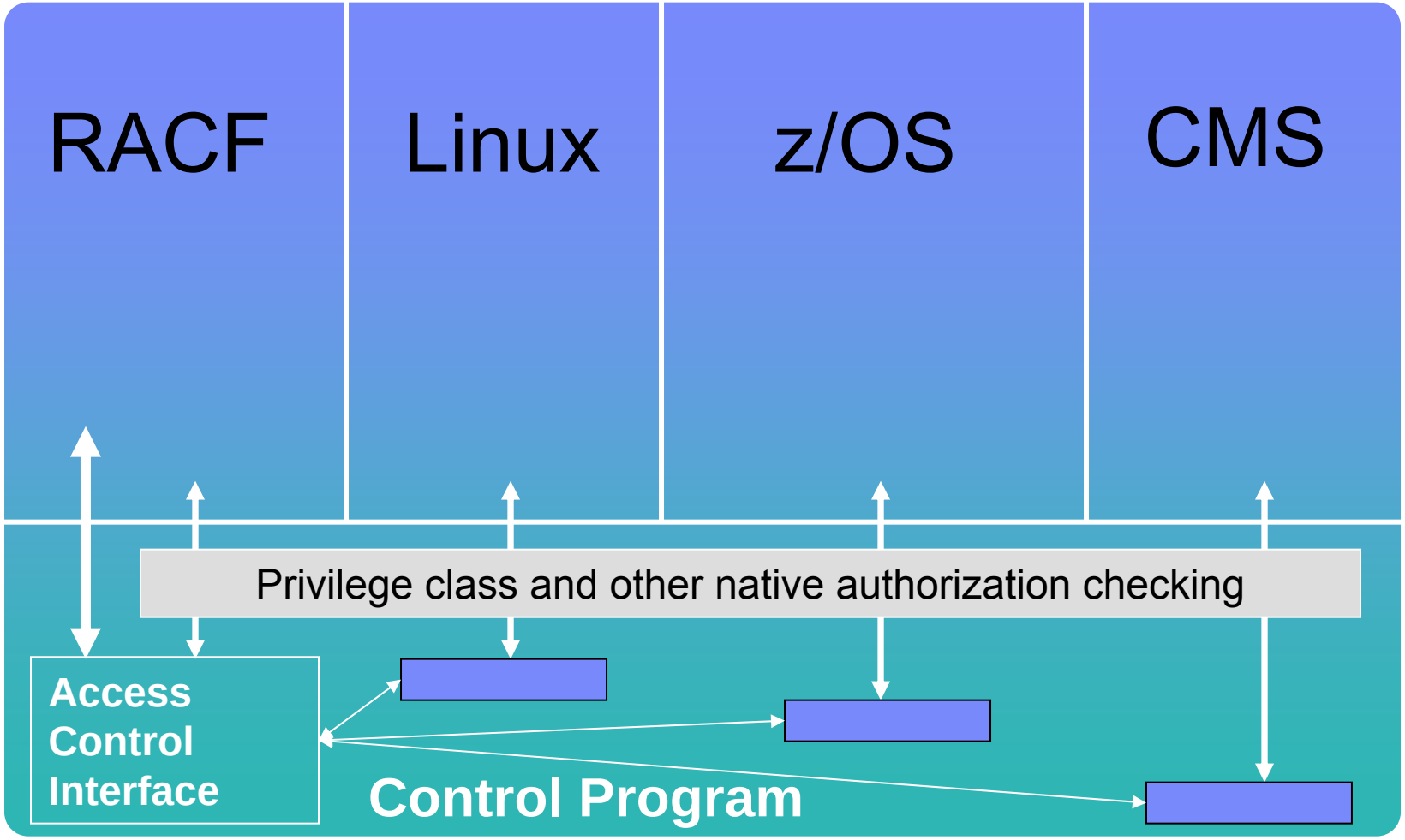
"It is clear that with the increase in popularity, relevance and deployment of virtualization starting in 2006, vulnerability discovery energies have increasingly focused on finding ways to exploit virtualization technologies."

"...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

z/VM Security Architecture

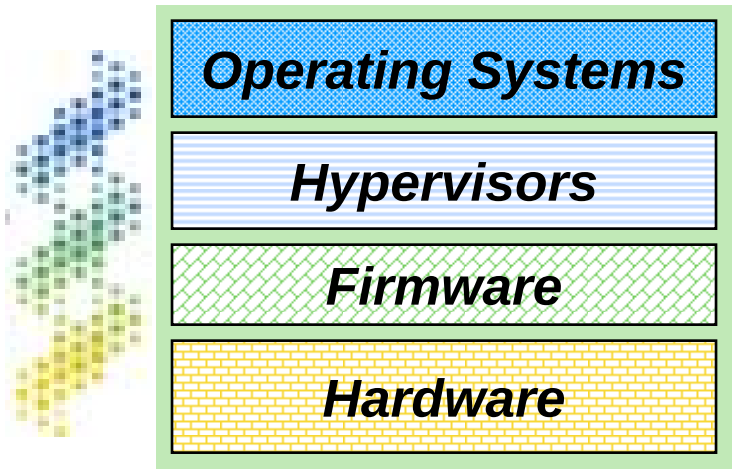


Topics

- Business drivers for server consolidation
- **System z: wired for virtualization**
- System z workload management: what every business needs
- Saving money, growing your business

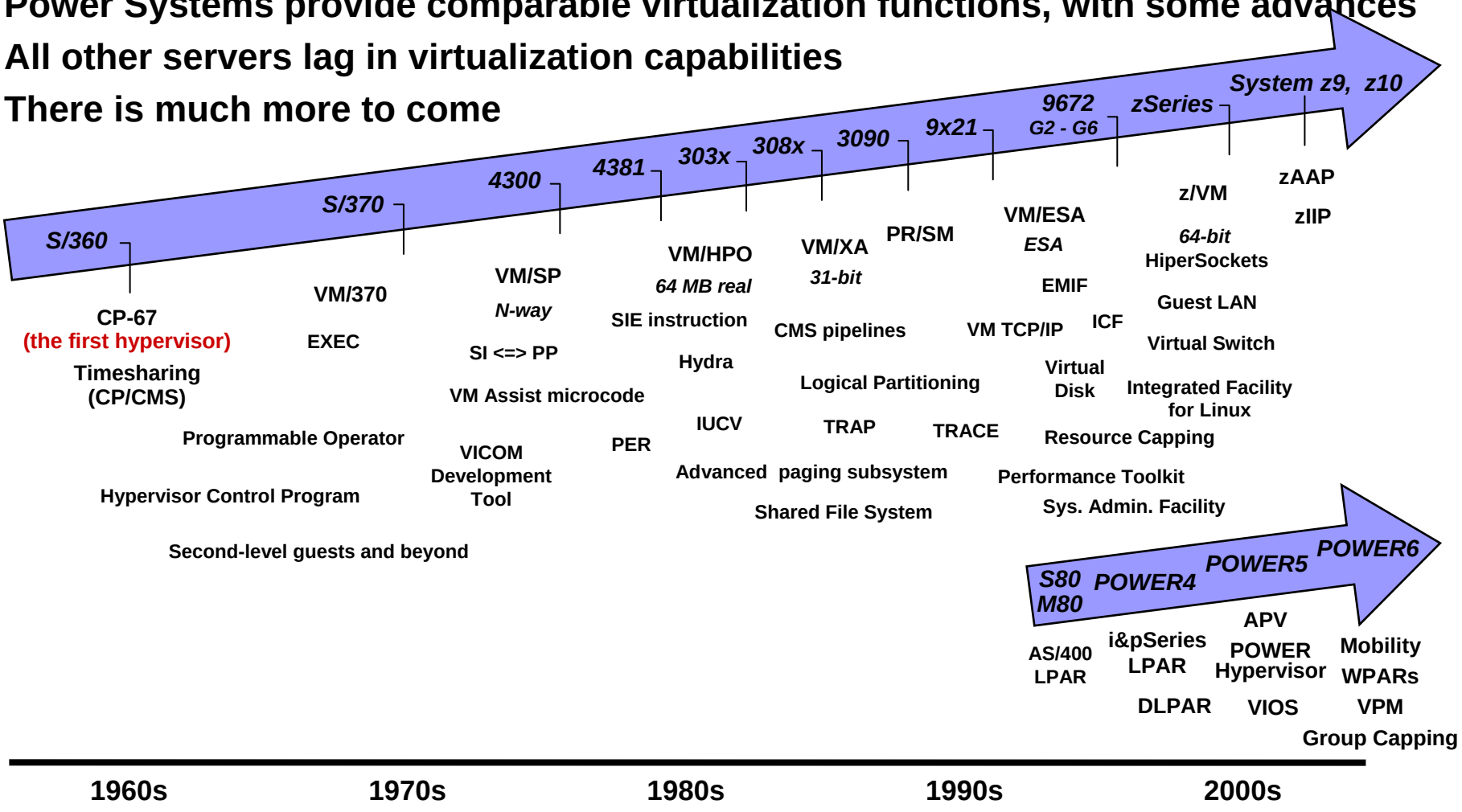
IBM System z Virtualization Genetics

- **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**



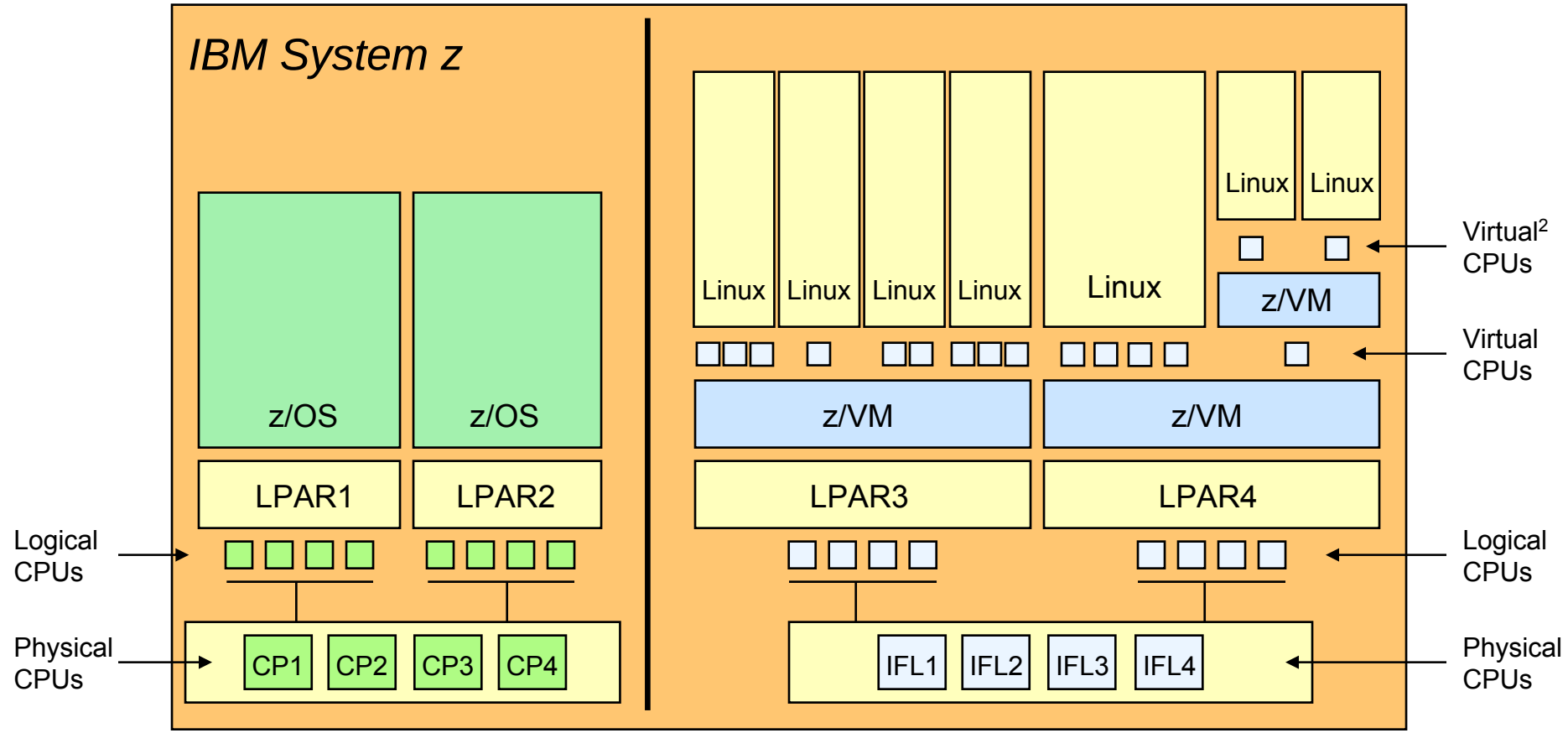
Forty Years of Continuing Innovation

- **Virtualization was pioneered and perfected on IBM mainframes**
- **System z continues to set the gold standard in server virtualization**
- **Power Systems provide comparable virtualization functions, with some advances**
- **All other servers lag in virtualization capabilities**
- **There is much more to come**



IBM System z Virtualization Leadership

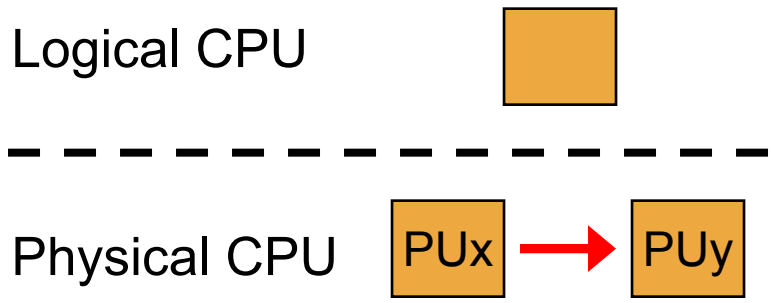
Extreme Levels of CPU Sharing

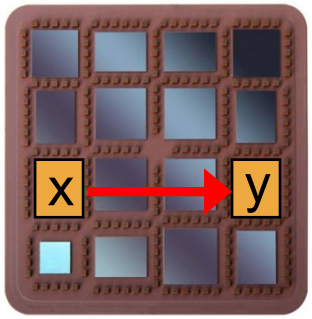


IBM System z CPU High Availability

Concurrent Processor Reassignment

- **Used to concurrently change the physical backing of one or more logical processors**
- **The state of source physical processor is captured and transplanted into the target physical processor**
- **Operation is transparent to operating systems**
- **Used for *processor sparing* and *book replacement***

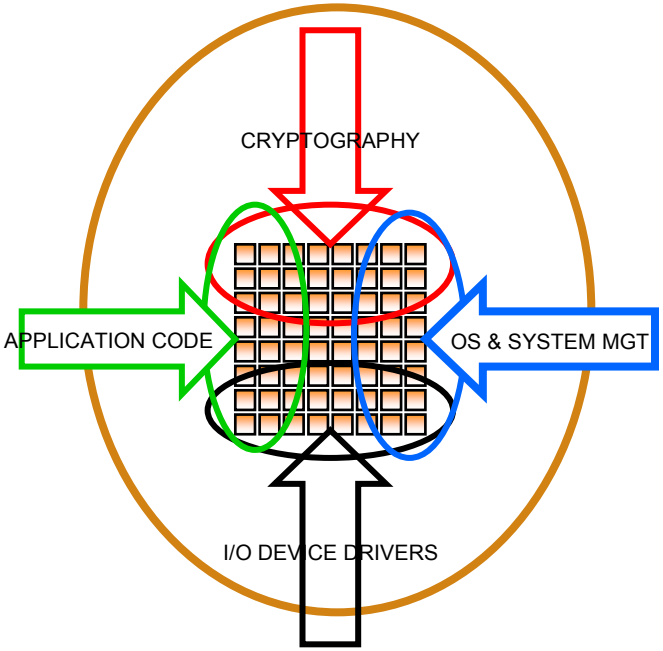




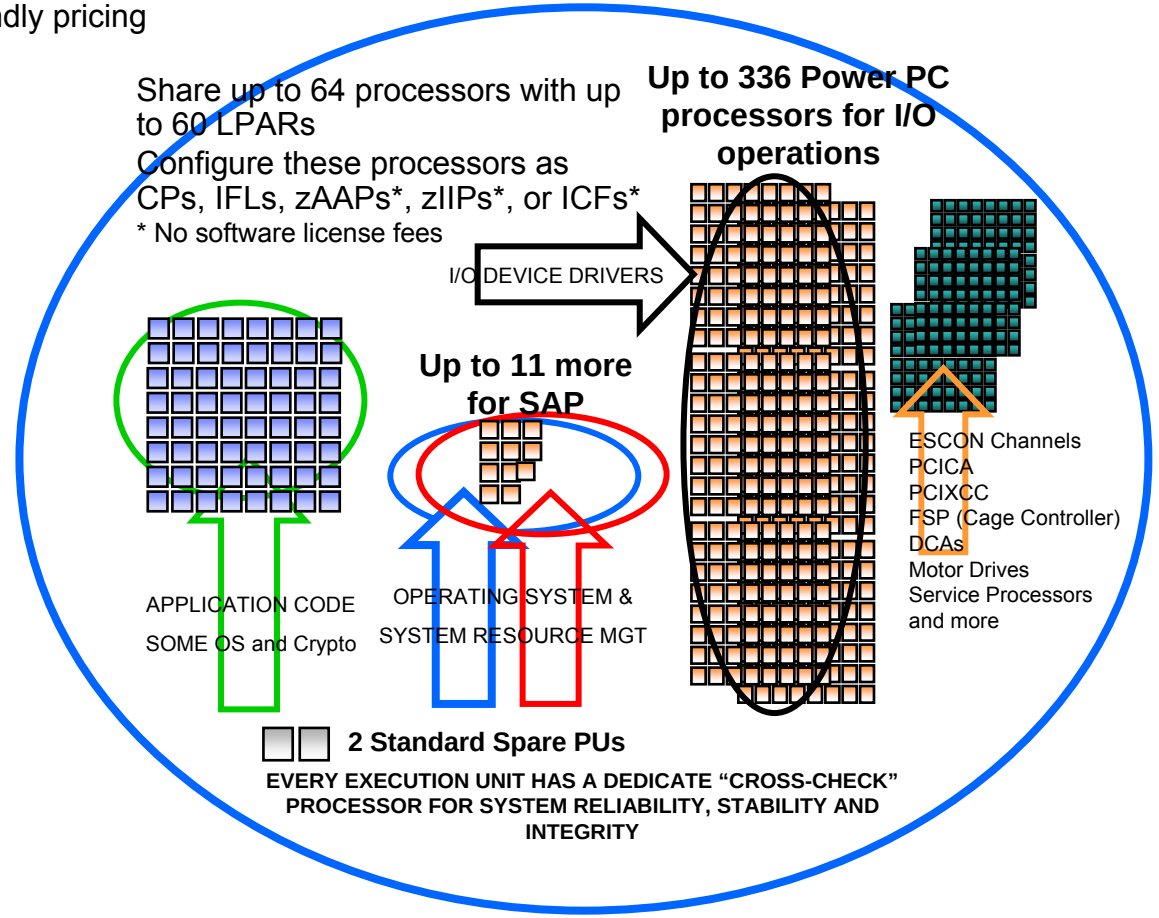
System Design Affects Virtualization Capabilities

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

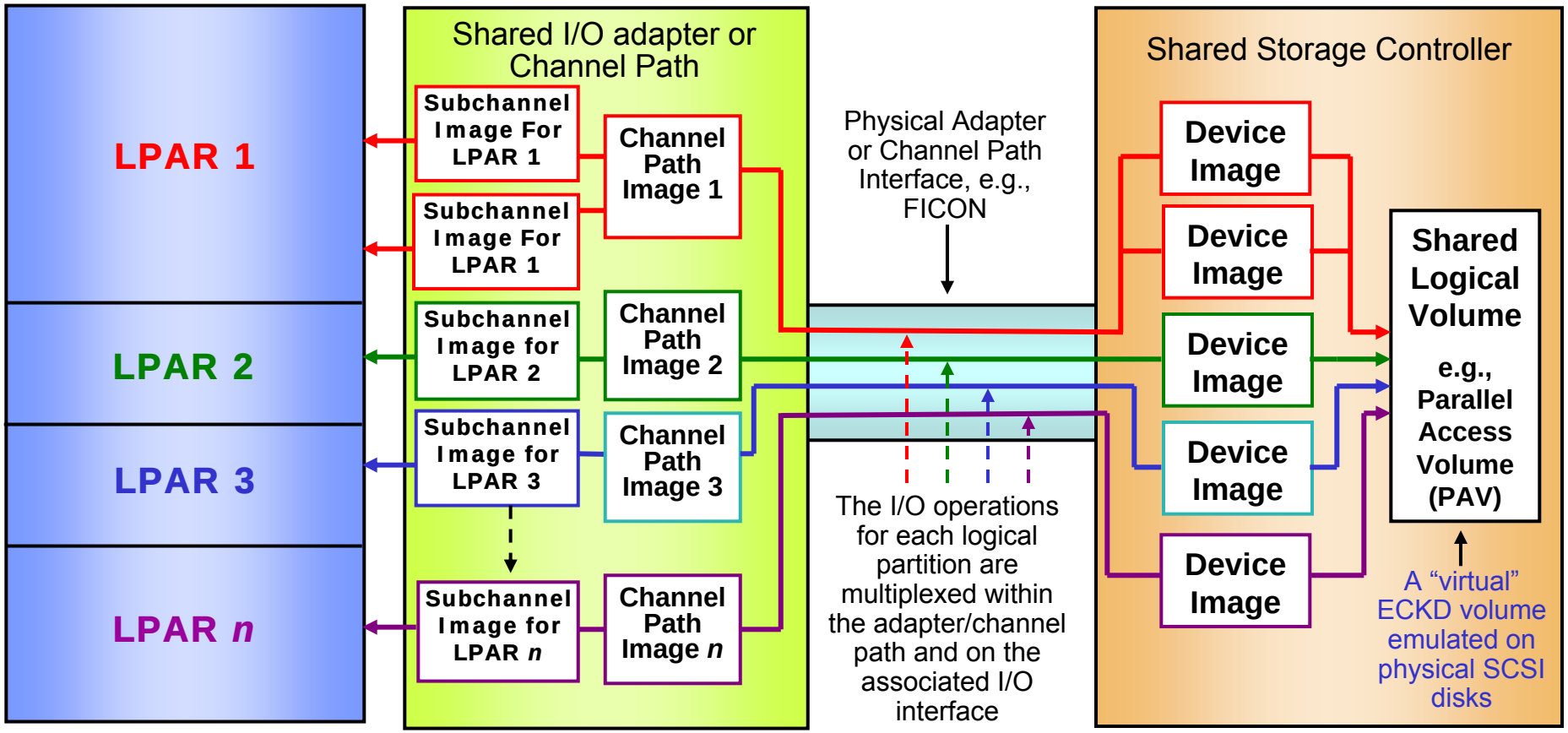
Tuned for "Jaw-Dropping" performance on industry standard benchmarks

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

PR/SM High-Performance I/O Sharing (Multi-Image Facility)

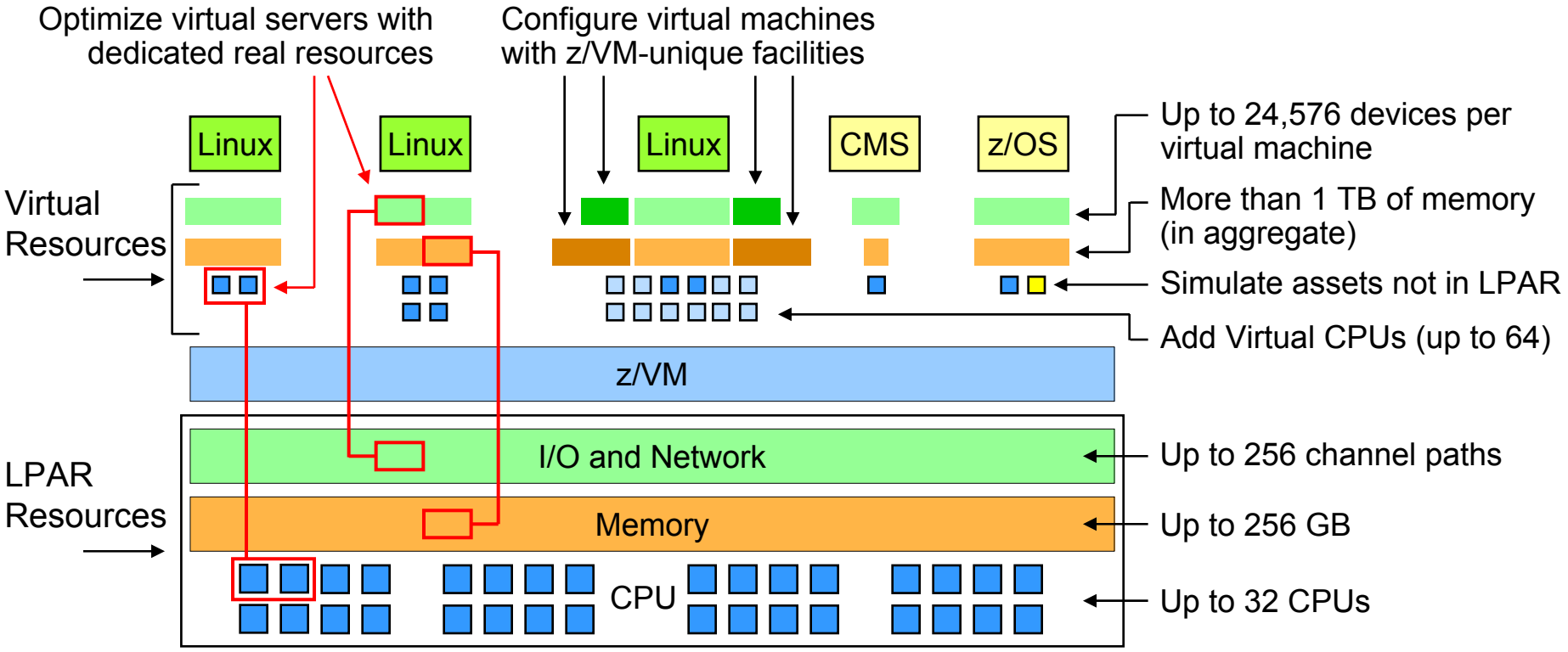


- The I/O infrastructure is shared by LPARs at native speeds, without hypervisor involvement
- Up to 8 physical channels process the I/O requests to the shared devices
  - This reduces the possibility of I/O queuing delays at the channels or at the shared storage controller

Extreme Virtualization with z/VM V5.4

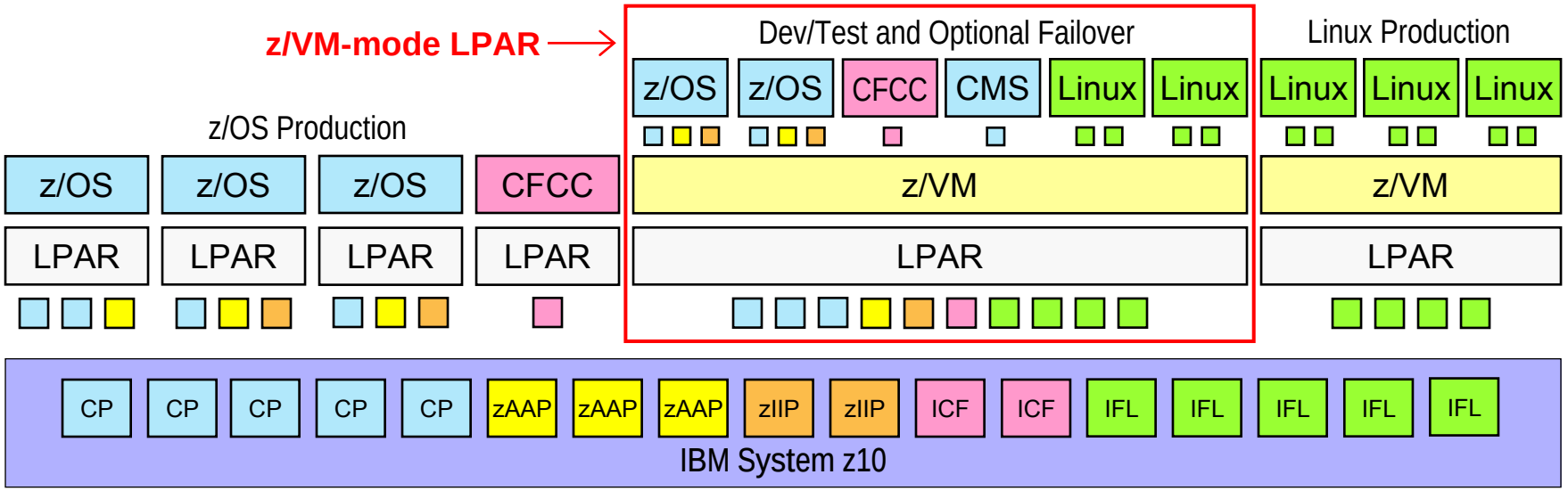
z/VM can massively scale a virtual server environment with a mix of virtual and real resources for each virtual machine

- With exceptional levels of performance, availability, and security
- Virtual and real assets can be non-disruptively added when needed



z/VM-Mode LPAR Support for IBM System z10

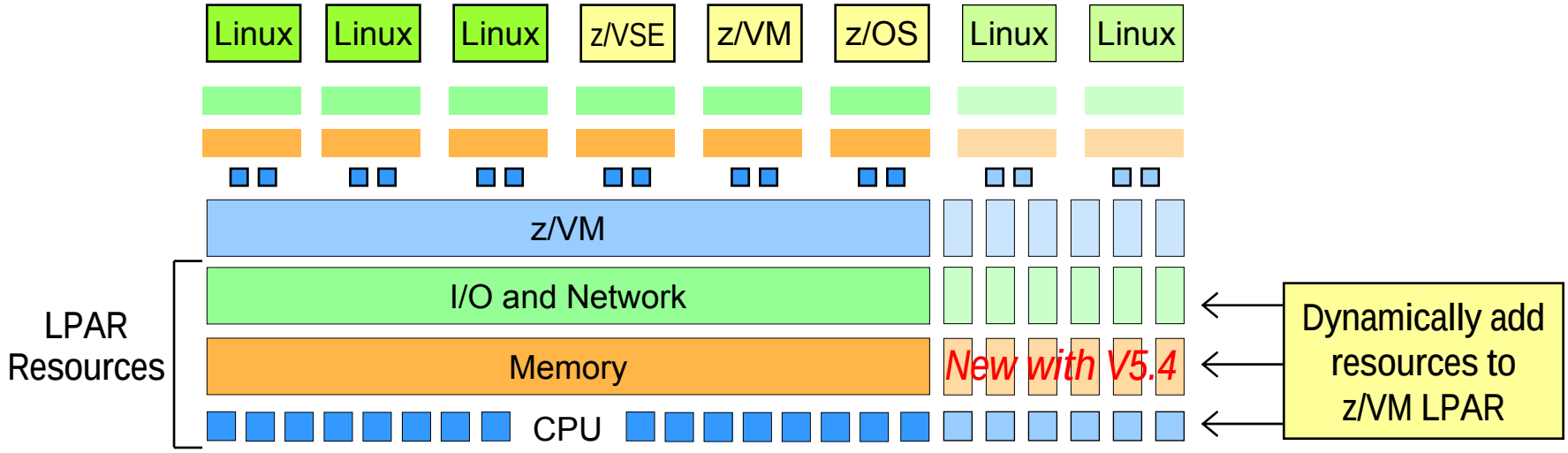
- **New LPAR type for IBM System z10: *z/VM-mode***
  - Allows z/VM V5.4 users to configure all CPU types in a z10 LPAR
- **Offers added flexibility for hosting mainframe workloads**
  - Add *IFLs* to an existing standard-engine z/VM LPAR to host Linux workloads
  - Add *CPs* to an existing IFL z/VM LPAR to host z/OS, z/VSE, or traditional CMS workloads
  - Add *zAAPs* and *zIIPs* to host eligible z/OS specialty-engine processing
  - Test integrated Linux and z/OS solutions in the same LPAR
- **No change to software licensing**
  - Software continues to be licensed according to CPU type



z/VM Dynamic Memory Upgrade

New z/VM V5.4 Function Enhances System Availability

- **Users can non-disruptively add memory to a z/VM *LPAR***
  - Additional memory can come from: *a)* unused available memory, *b)* concurrent memory upgrade, or *c)* an LPAR that can release memory
  - Memory *cannot* be non-disruptively removed from a z/VM LPAR
- **z/VM virtualizes this hardware support for *guest machines***
  - Currently, only z/OS and z/VM support this capability in a virtual machine environment
- **Complements ability to <u>dynamically</u> add CPU, I/O, and networking resources**

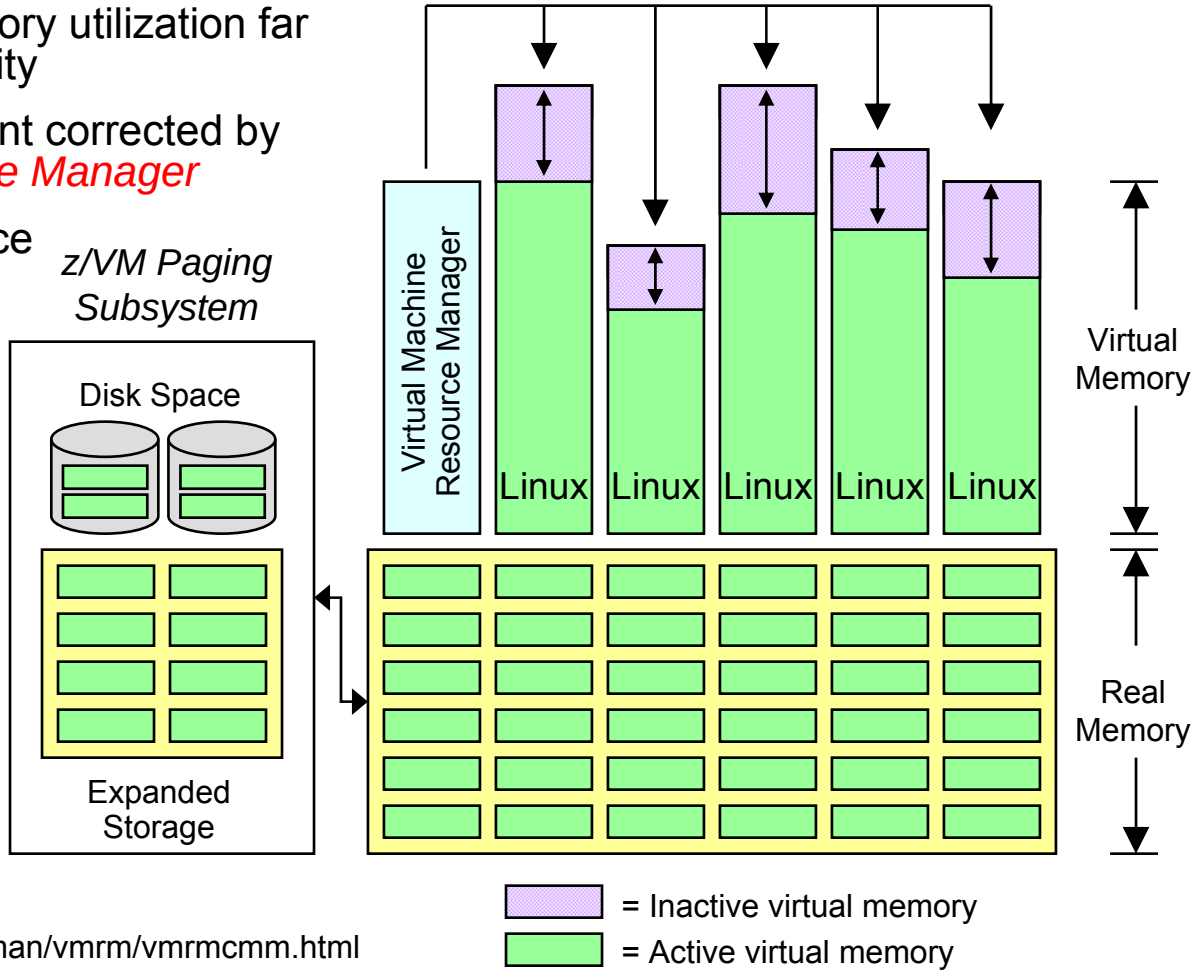


Smart economics: non-disruptively scale your z/VM environment by adding hardware assets that can be shared with every virtual server

Extreme Virtualization with Linux on z/VM

VMRM Cooperative Memory Management (VMRM-CMM)

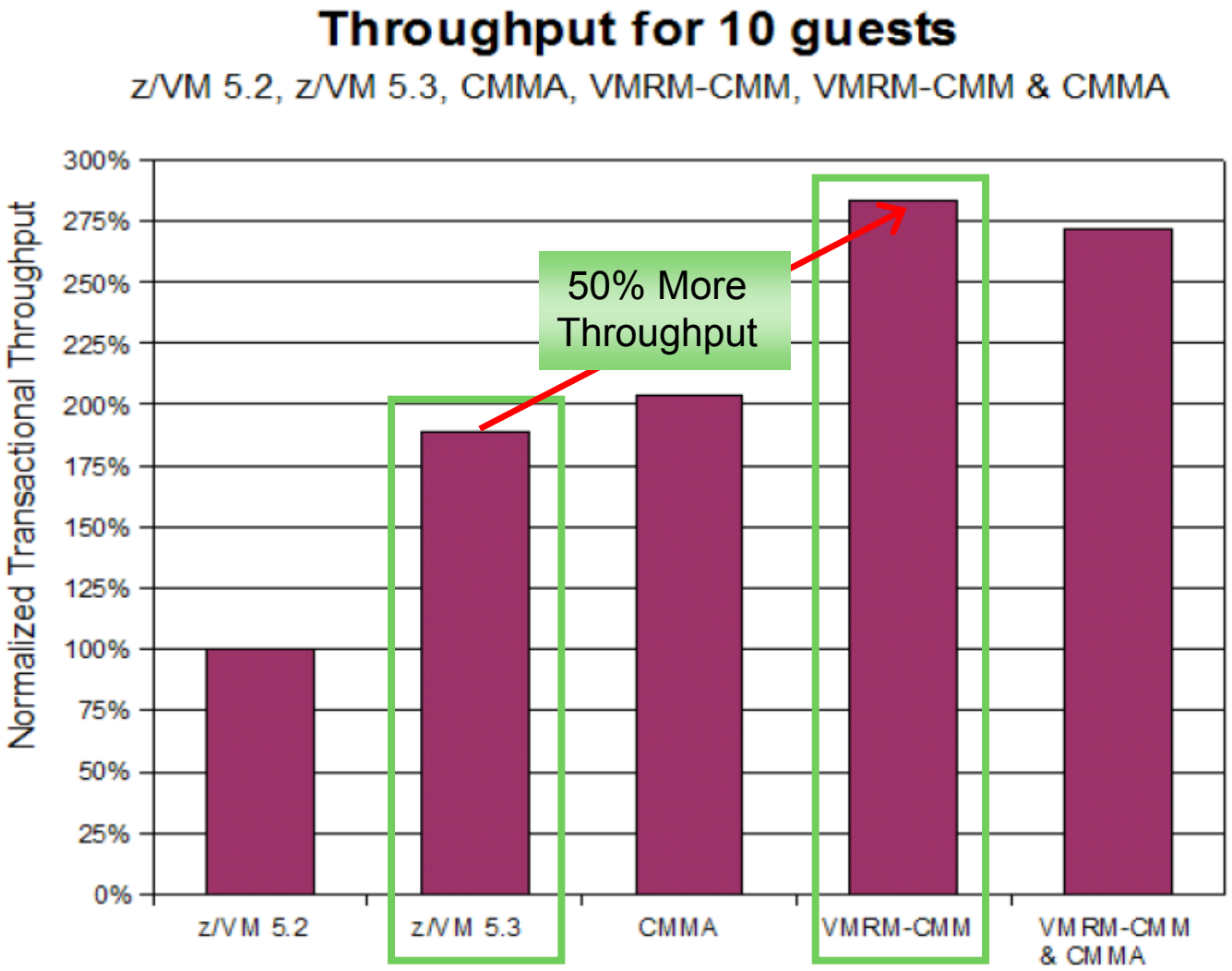
- Problem scenario: virtual memory utilization far exceeds real memory availability
- Solution: real memory constraint corrected by z/VM *Virtual Machine Resource Manager*
- Linux images signaled to reduce virtual memory consumption
- Demand on real memory and z/VM paging subsystem is reduced
- Helps improve overall system performance and guest image throughput



Learn more at:
ibm.com/servers/eserver/zseries/zvm/sysman/vmrm/vmrmcmm.html

OLTP Database Environment with VMRM-CMM and CMMA

Excerpt from "z/VM Large Memory – Linux on System z" Whitepaper

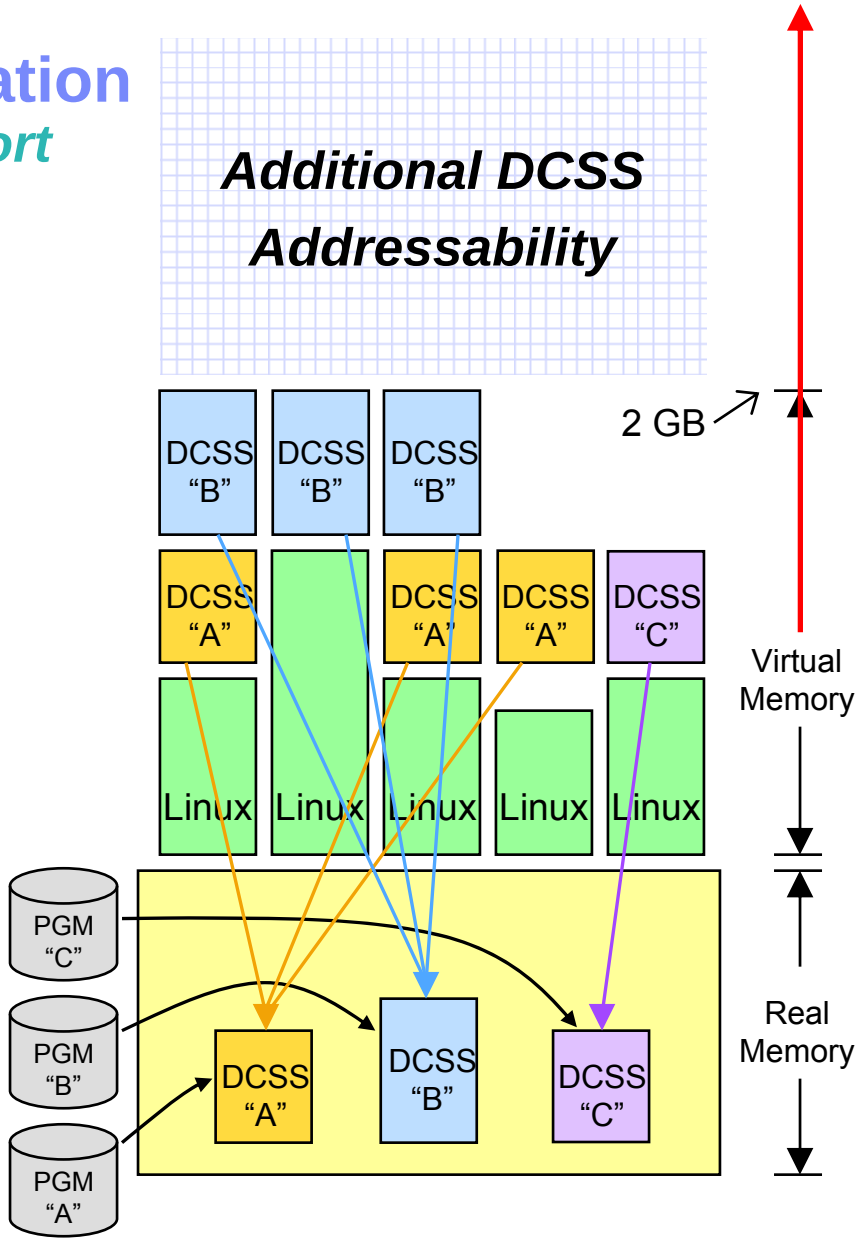


Extreme Linux-on-z/VM Virtualization

Linux Exploitation of z/VM DCSS Support

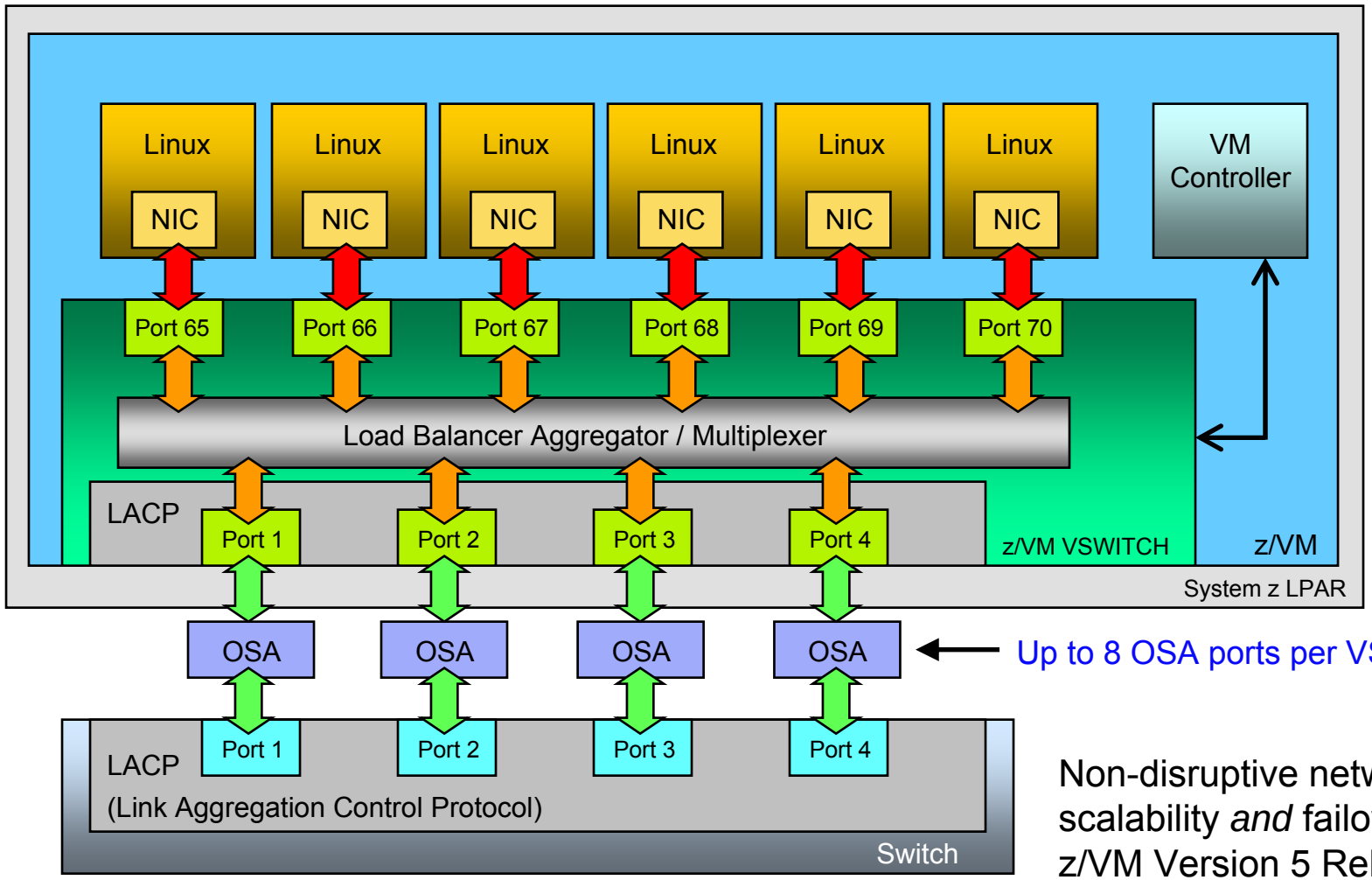
- Discontinguous Saved Segments (DCSS)
  - Share a single, real memory location among multiple virtual machines
  - Can reduce real memory utilization
- Linux exploitation: shared program executables
  - Program executables are stored in an execute-in-place file system, then loaded into a DCSS
  - DCSS memory locations can reside outside the defined virtual machine configuration
  - Access to file system is at memory speeds; executables are invoked directly out of the file system (no data movement required)
  - Avoids duplication of virtual memory
  - Helps enhance overall system performance and scalability
- **z/VM V5.4 support enhancements:**
  - Segments can reside above 2 GB address line
  - Enables even greater system scalability
  - New addressing limit is 512 GB

Note: Maximum size of a single DCSS is 2047 MB



z/VM Virtual Switch Link Aggregation Support

Enhanced Networking Bandwidth and Business Continuance



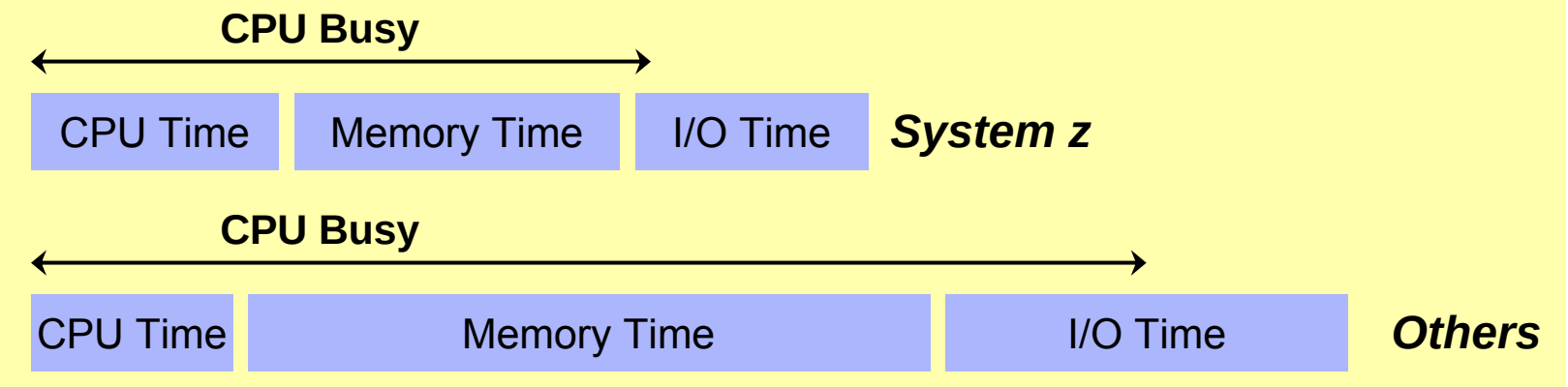
Non-disruptive networking scalability *and* failover with z/VM Version 5 Release 3

Note: Requires OSA-Express2 support available with IBM System z9 and later servers

What Kind of Workload Runs Best on Mainframes?

- **Consider *system* performance and capacity in selecting "best fit" for your applications**

  Data intensive workloads like large databases, transaction processing, object oriented code and context switching often run better on System z, due to its processor caching and I/O architecture.

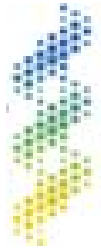


- **Also factor in the value derived from the co-residency of applications and data servers on a single mainframe**

Topics

- Business drivers for server consolidation
- System z: wired for virtualization
- **System z workload management: what every business needs**
- Saving money, growing your business

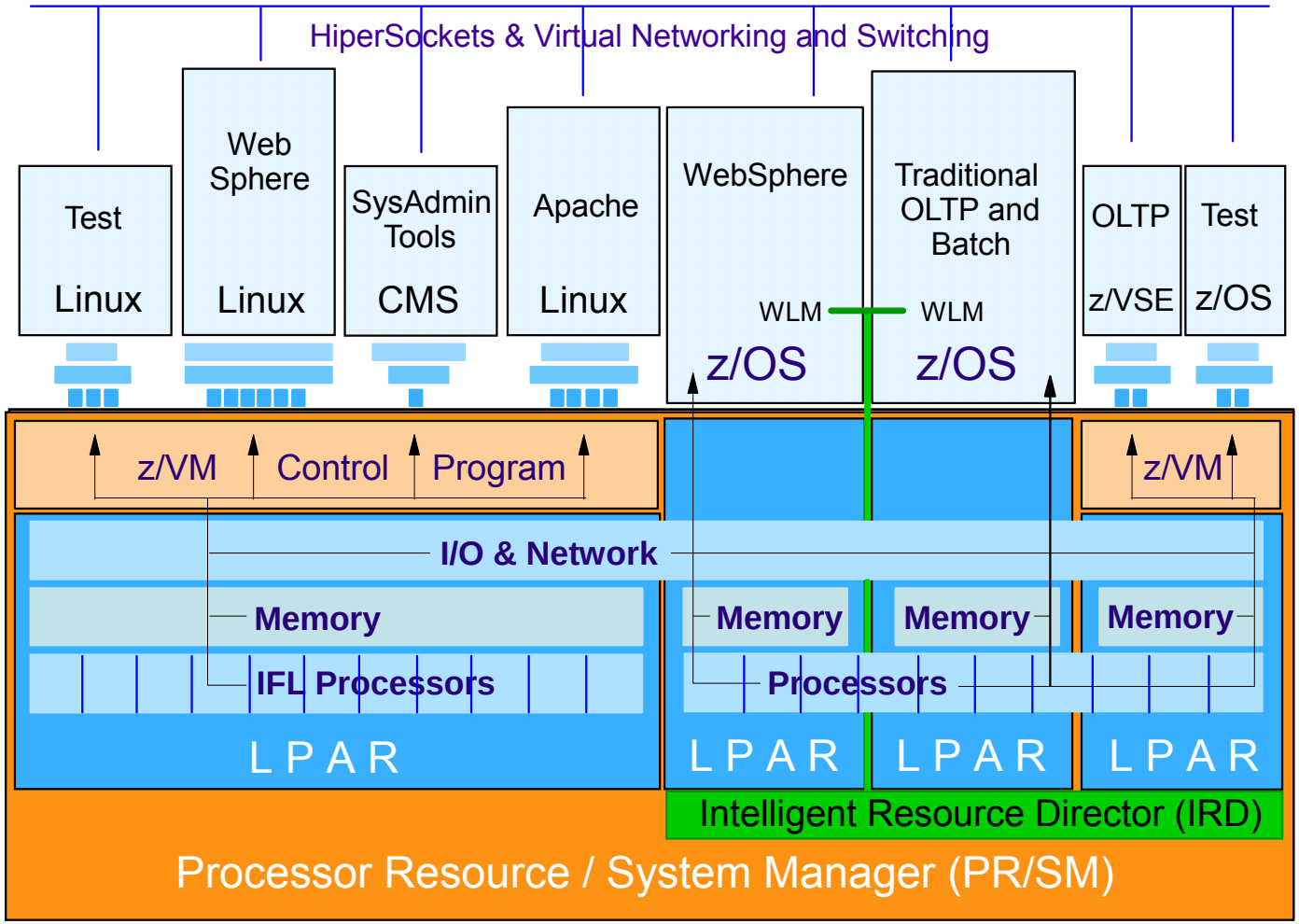
System z Workload Management



- **IBM System z workload management is expertly crafted to:**
  - Maximize the virtualization capabilities of an infrastructure already designed to share hardware assets
  - Align IT resources with business needs with a degree of certainty unmatched by other platforms
  - Minimize the time-consuming, low-value busy work associated with a server sprawl solution (e.g., “Security Tuesdays”)
  - Deliver tangible cost savings to the bottom line
    - Software license fees
    - Staff productivity
    - Cost-efficient support for business continuance

IBM System z Virtualization Workload Management

The Big Picture



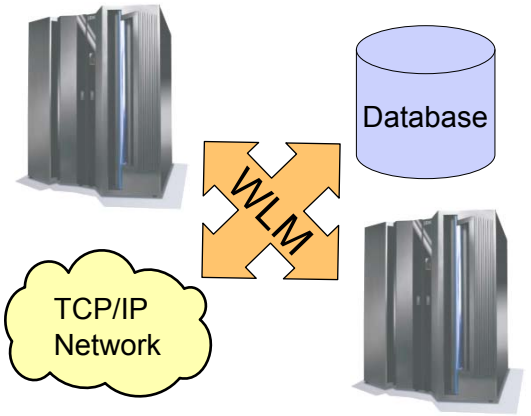
Multi-dimensional virtualization technology

- PR/SM enables highly scalable virtual server hosting for LPAR *and* z/VM virtual machine environments
- IRD coordinates allocation of CPU and I/O resources among z/OS and non-z/OS LPARs*
- Ideally suited for large-scale hosting of mixed workloads

* Excluding non-shared resources like Integrated Facility for Linux processors

z/OS Workload Management

Prioritizing work in a single z/OS image, across LPARs, across a Parallel Sysplex, to your network



- Define performance goals in business terms and assign importance to each goal: manage to service level agreements
- The system decides how much resource is needed to meet the goals
- Resources are shared dynamically across mixed applications
- End-to-end prioritization capability, from the network to the data
- Workload Manager will monitor the system and adjust processing to meet the goals

With z/OS 1.8: more integration with EWLM (Enterprise Workload Manager), facilitating the end-to-end management of workloads.

A History of Advanced Technology	
Workload Manager (WLM)	1994
Parallel Sysplex	1994
Sysplex Data Sharing	1994
TCP/IP Sysplex Distributor	2000
Intelligent Resource Director (IRD)	2001
Transactional VSAM (DFSMStvs)	2002
TCP/IP Sysplex Health Monitoring	2004
Cross platform monitoring (EWLM)	2004
WebSphere Application Server	2004
DB2 Stored Procedures / Latches	2005
Sysplex Distributor Coordination	2005
Load Balancing Advisor	2005
Support for zAAP	2005
Group Capacity Limits	2006
Support for zIIP	2007

Topics

- Business drivers for server consolidation
- System z: wired for virtualization
- System z workload management: what every business needs
- **Saving money, growing your business**

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

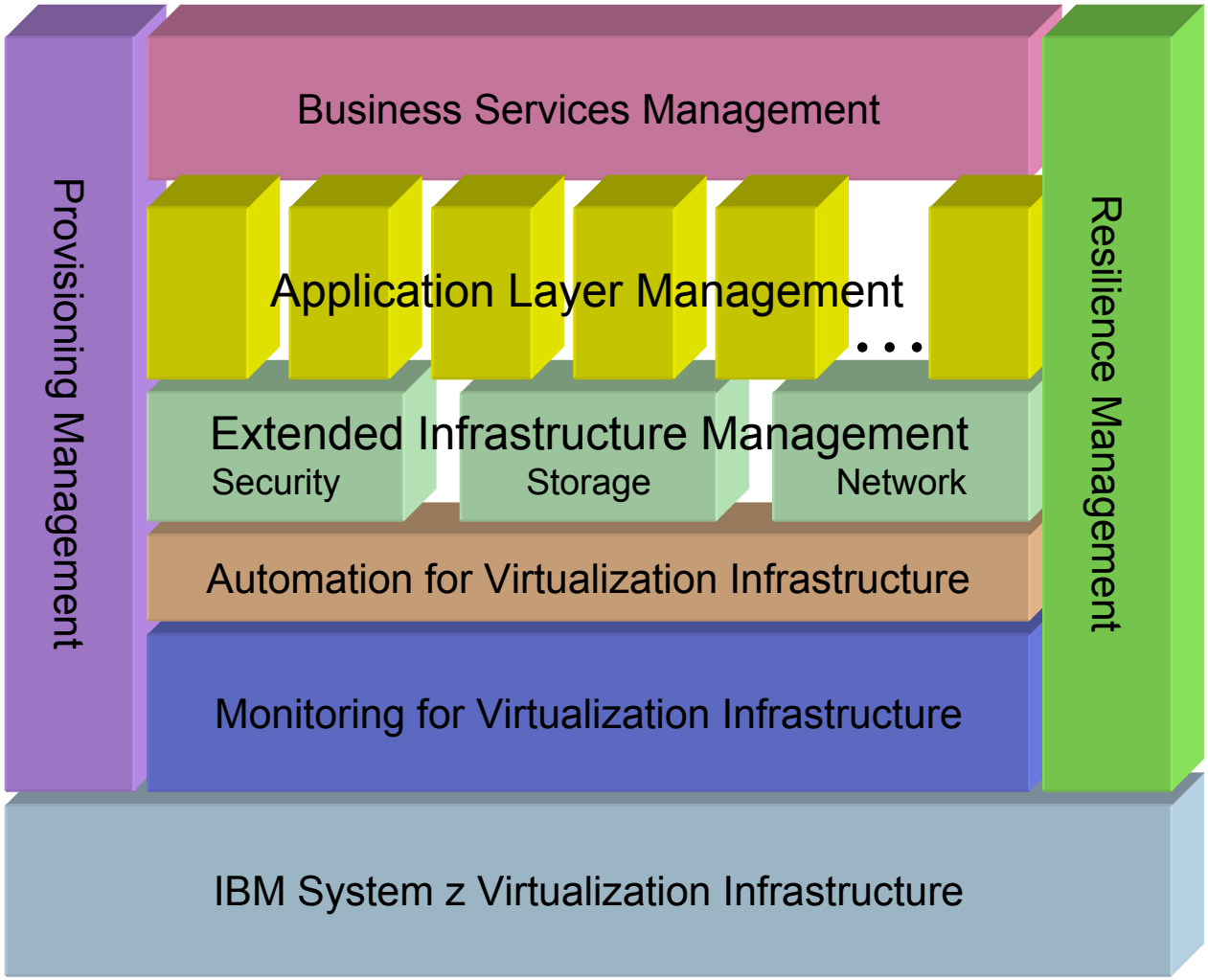
Helps secure your virtual servers and reduce business risk

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

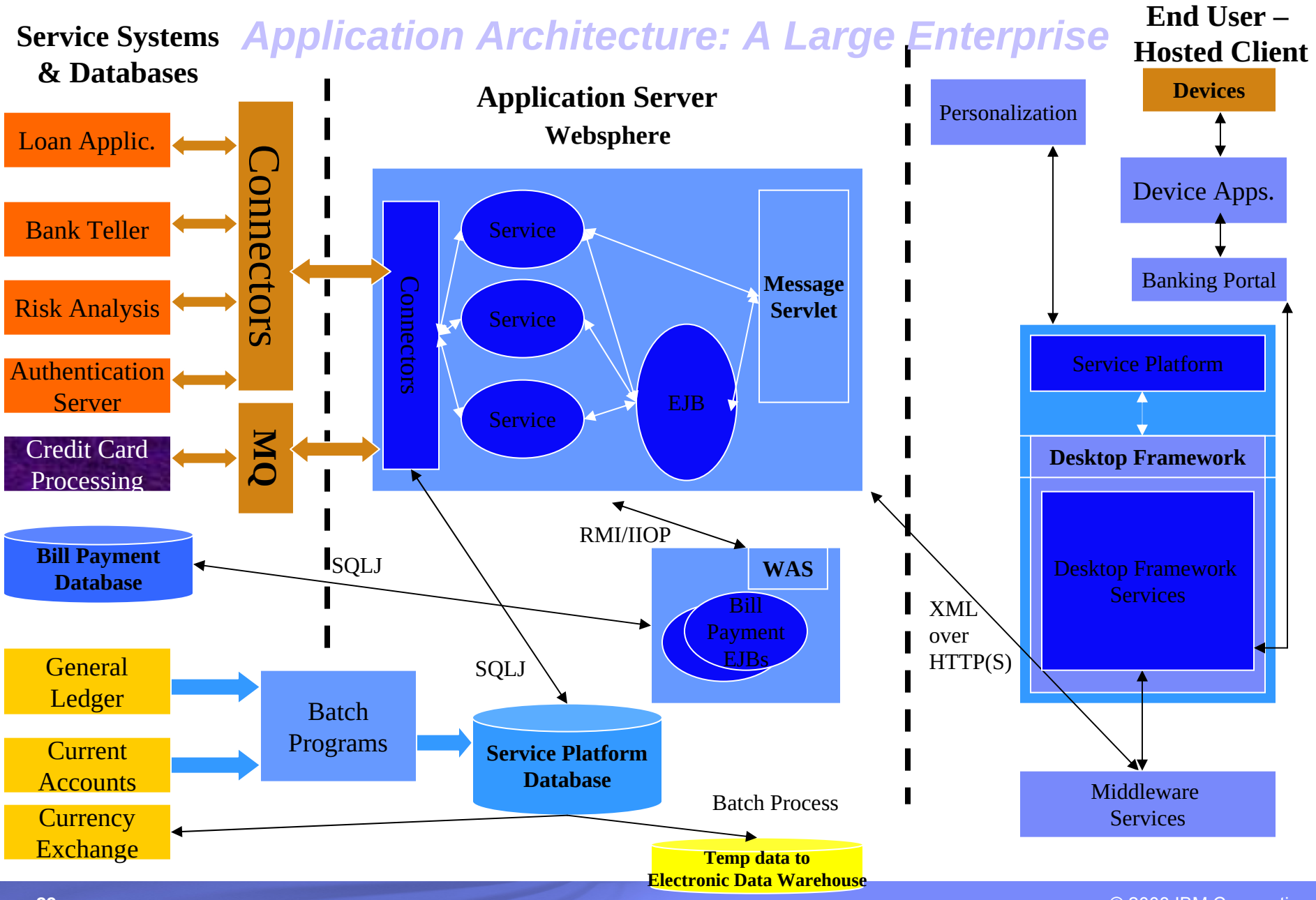
Increase staff productivity and virtualize the enterprise

IBM Tivoli Virtualization Management for System z

Helping Clients Manage and Control Their Virtualized IT Infrastructure

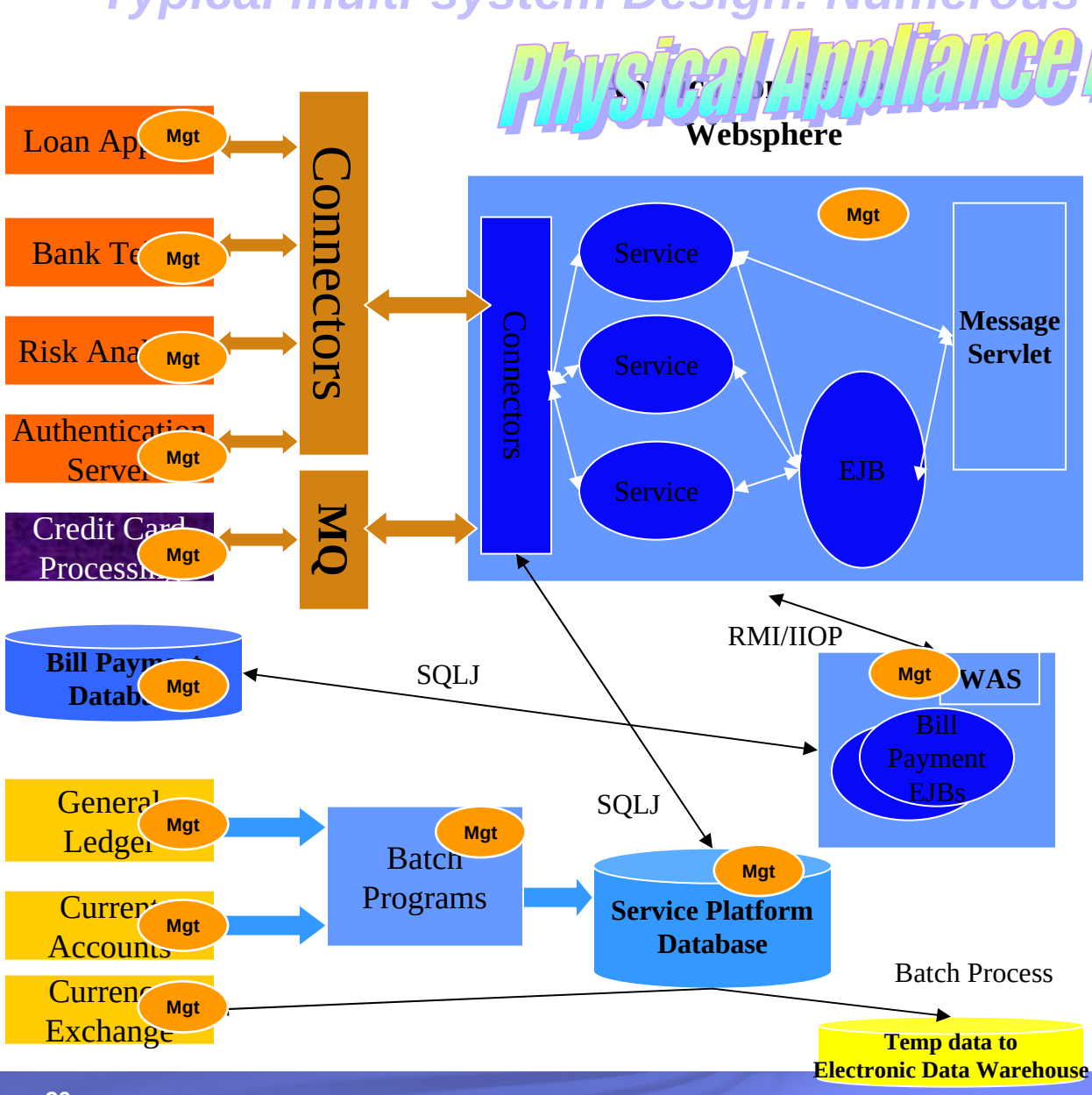


Application Architecture: A Large Enterprise



Typical multi-system Design: Numerous Mgmt Domains

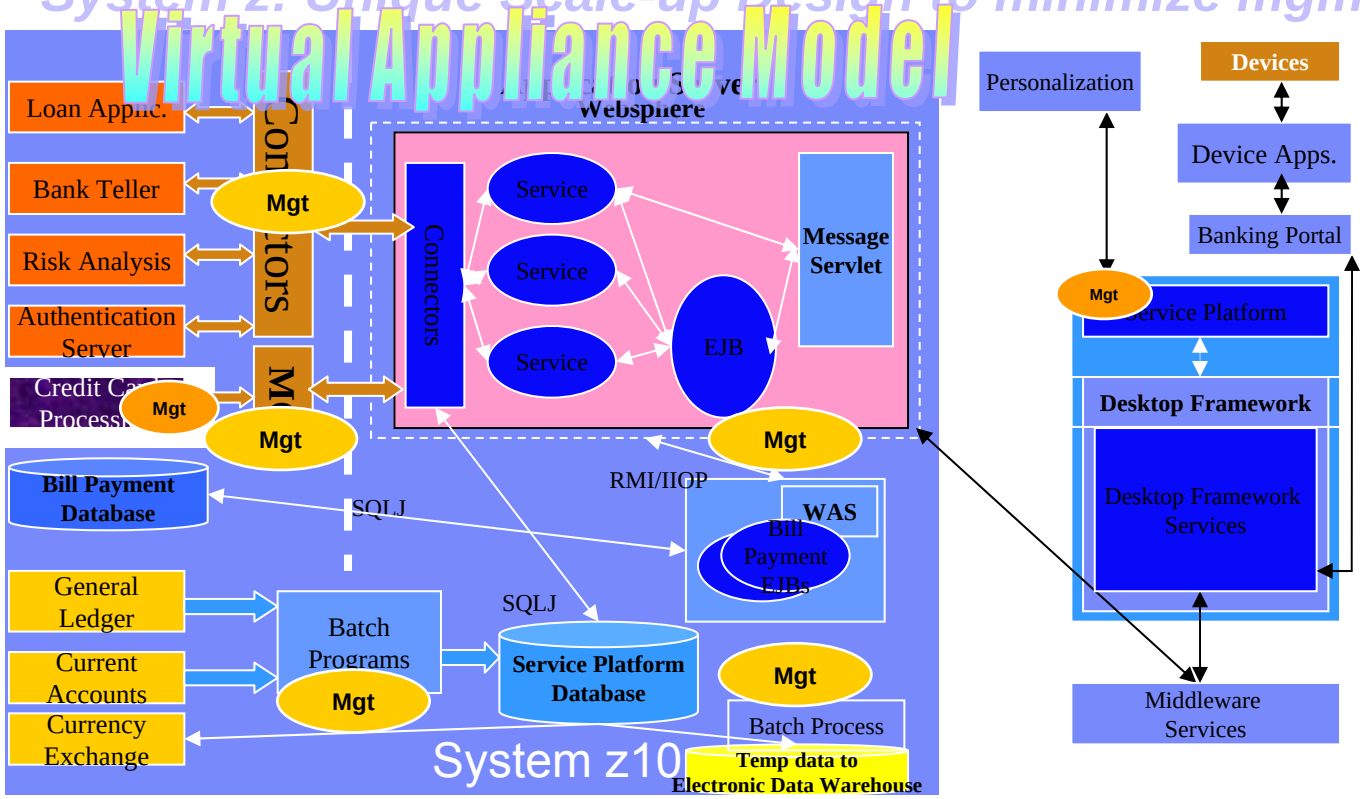
Physical Appliance Model



- 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

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

Virtual Appliance Model



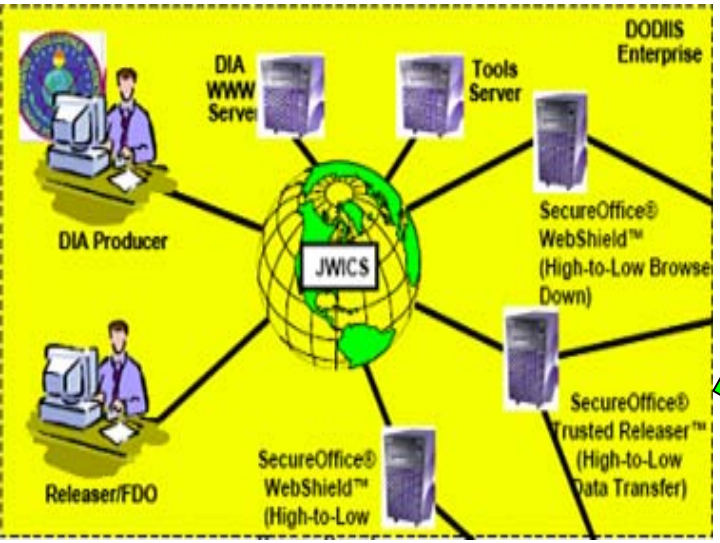
Potential advantages of consolidating your application and data serving

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

Secure Virtualization Changes Operational Model

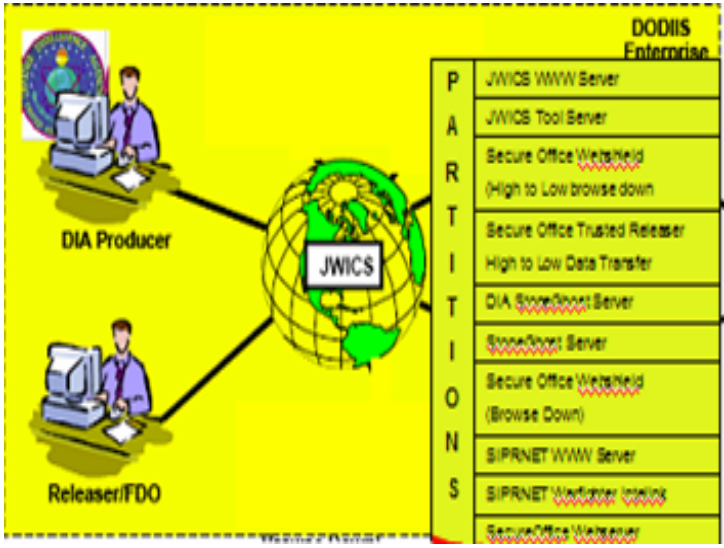


Opportunities for Cost Savings

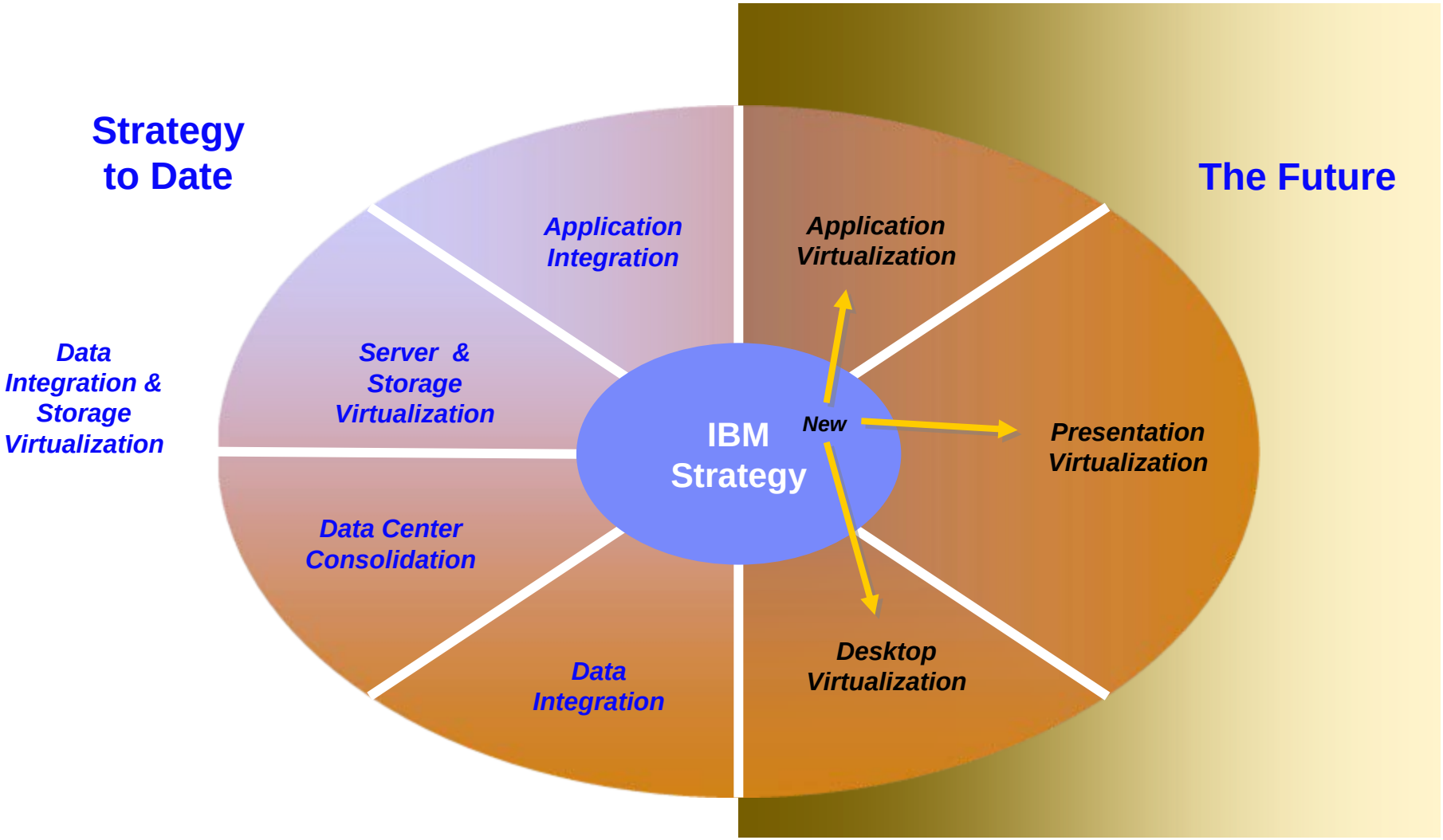
- Overcommitment of CPU resources can reduce software license fees
- Large-scale virtual server deployment on a single z/VM hypervisor can greatly enhance staff productivity
- Reliability and redundancy of System z infrastructure helps lessen application outages
- Flexible configuration options for business 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)



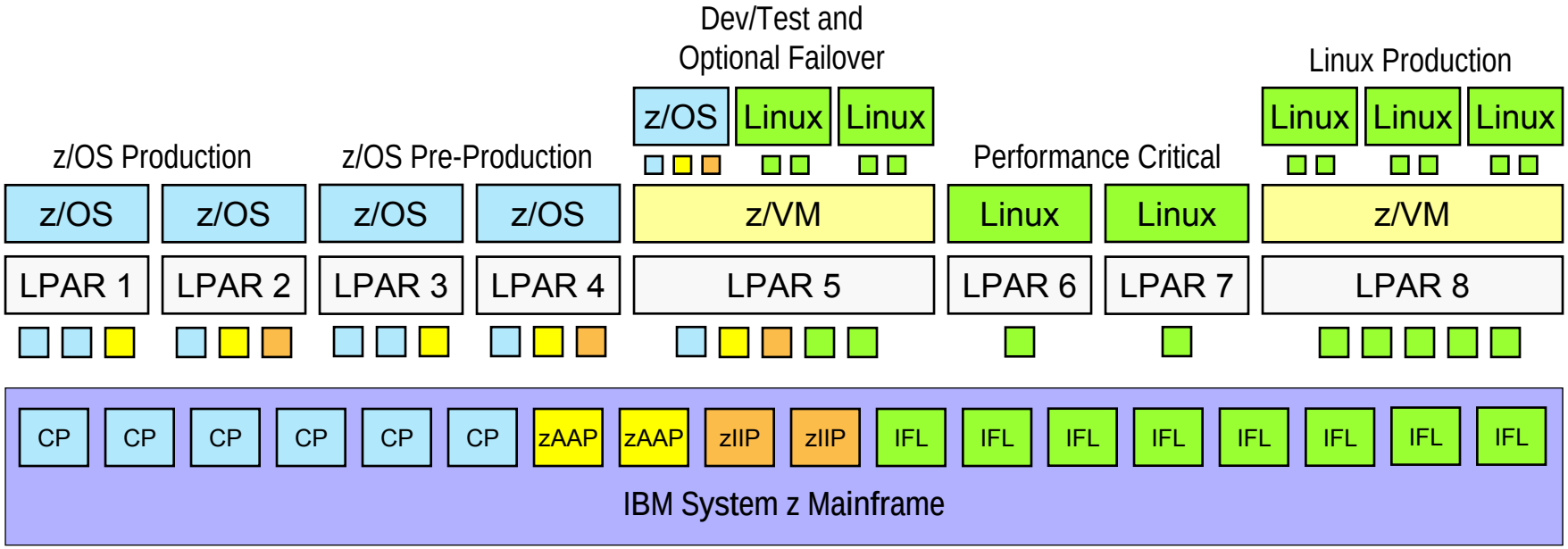
Extreme Virtualization with System z
Understanding the Value Proposition

- **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

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)



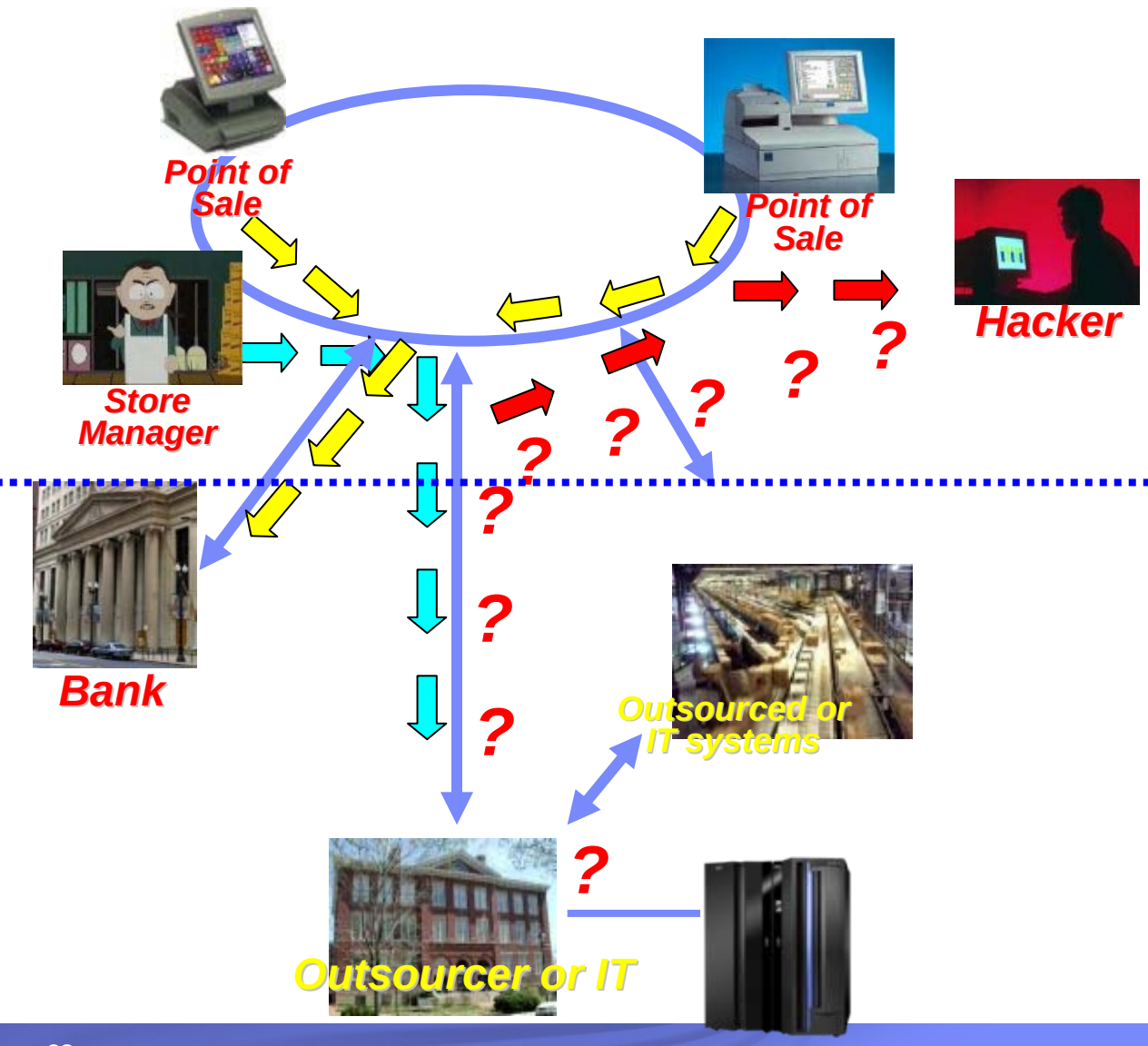
Questions

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

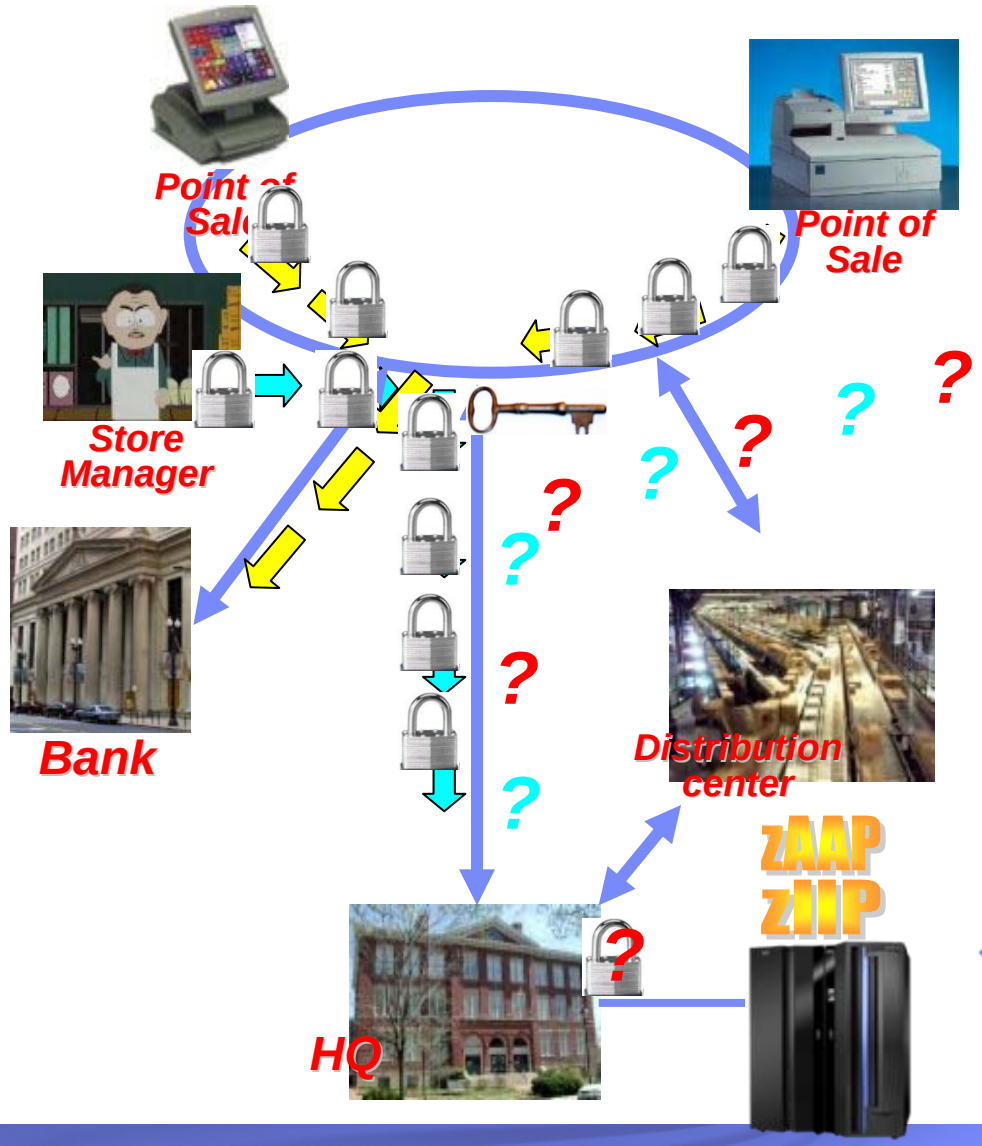
PCI DSS Ver. 1.1

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

IBM Global Services: Security & Privacy Consulting

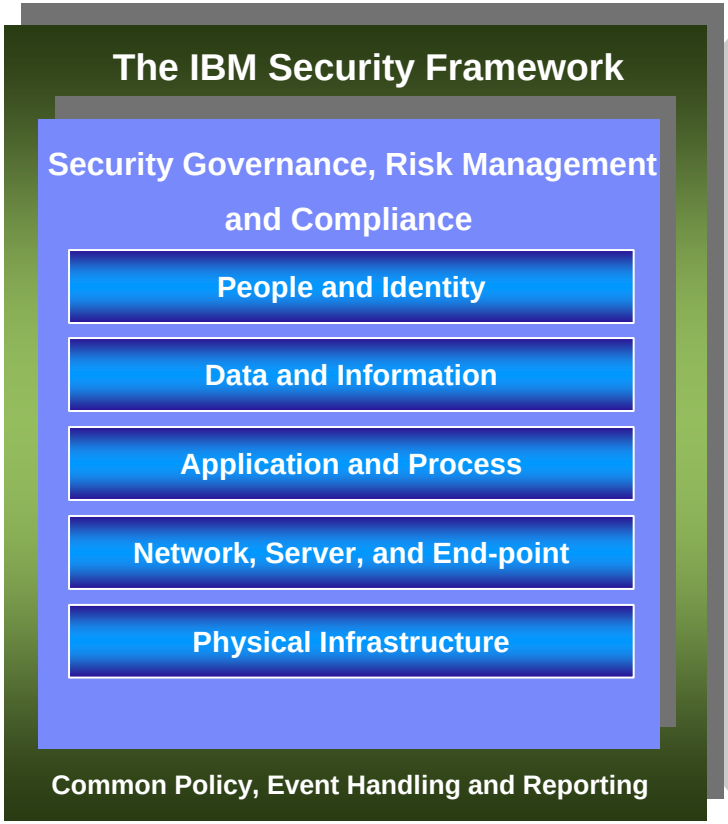
VENAFI

Intellinx
A Breakthrough in Insider Threat Detection & Prevention

IBM Business Partner

Tivoli. Compliance Insight Manager

IBM Security Framework



IBM Security Solutions

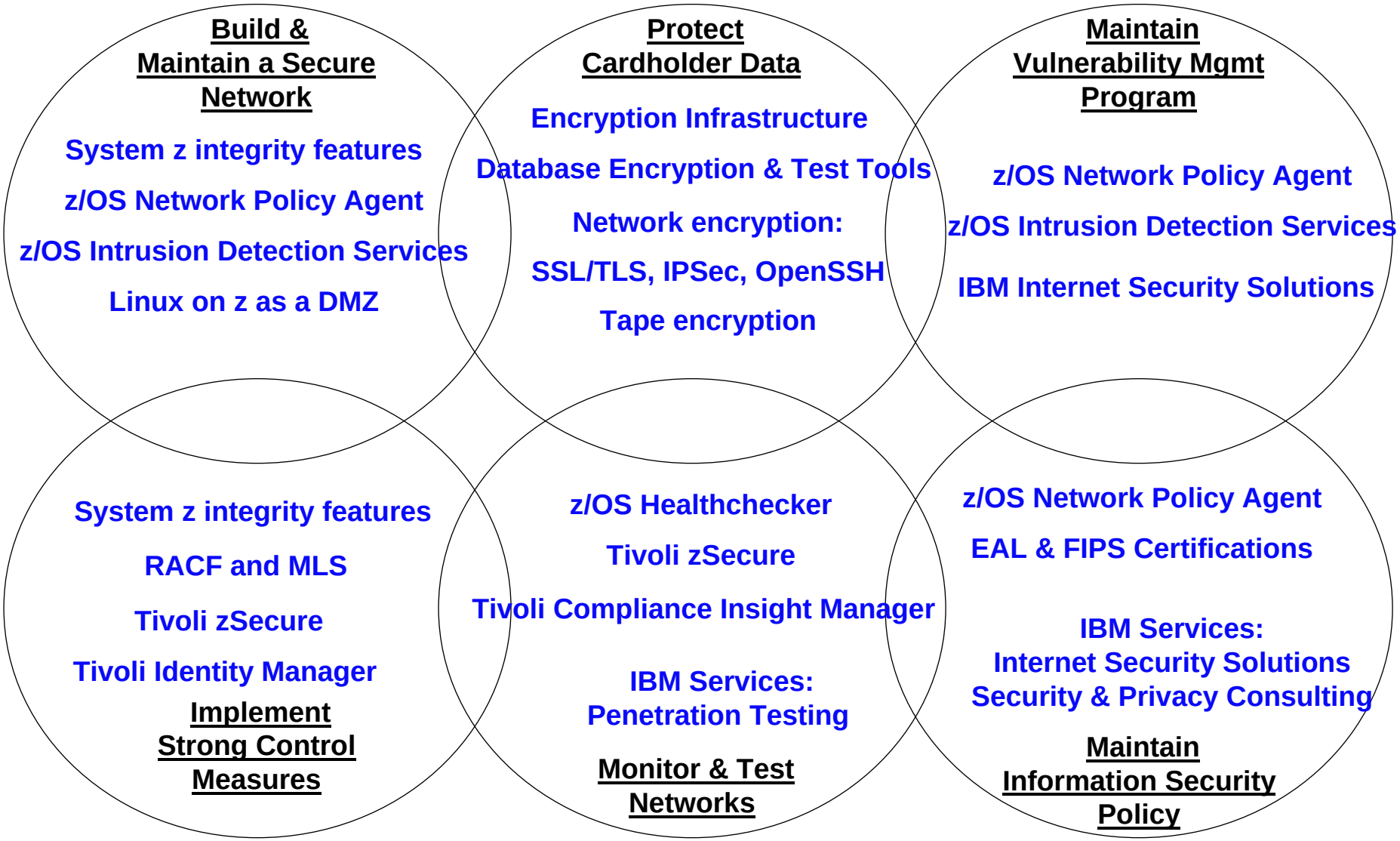
- SECURITY COMPLIANCE
  - Demonstrable policy enforcement aligned to regulations, standards, laws, agreements (PCI, FISMA, etc..)
- IDENTITY & ACCESS
  - Enable secure collaboration with internal and external users with controlled and secure access to information, applications and assets
- DATA SECURITY
  - 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 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's History in Security Technology

- **IBM Common Cryptographic Architecture CCA**
- **Lucifer II (Feistel 1975) and Date 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)***

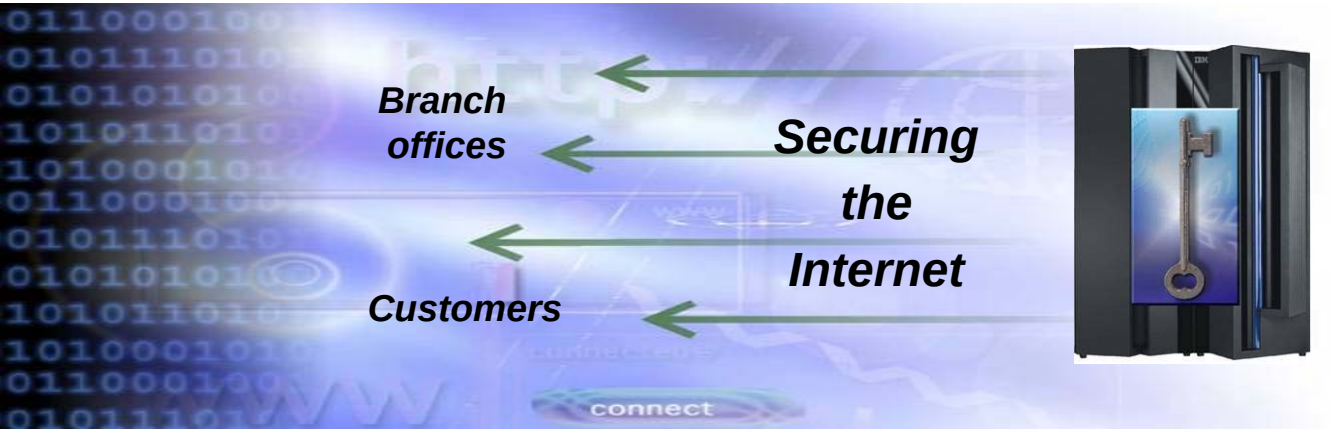
Payment Card Industry Compliance– How System z can help



*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.

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

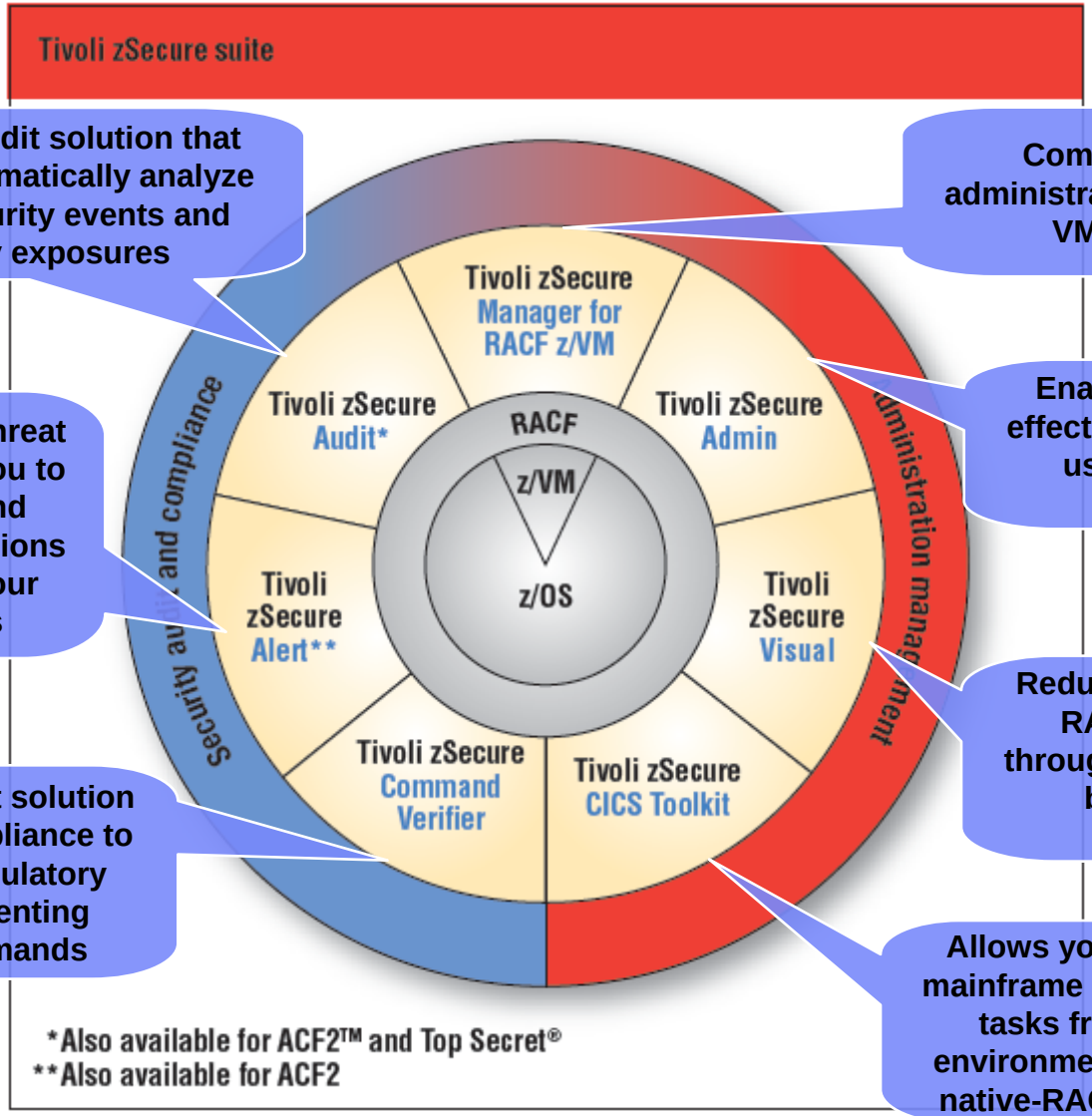


BANCO DO BRASIL

- **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

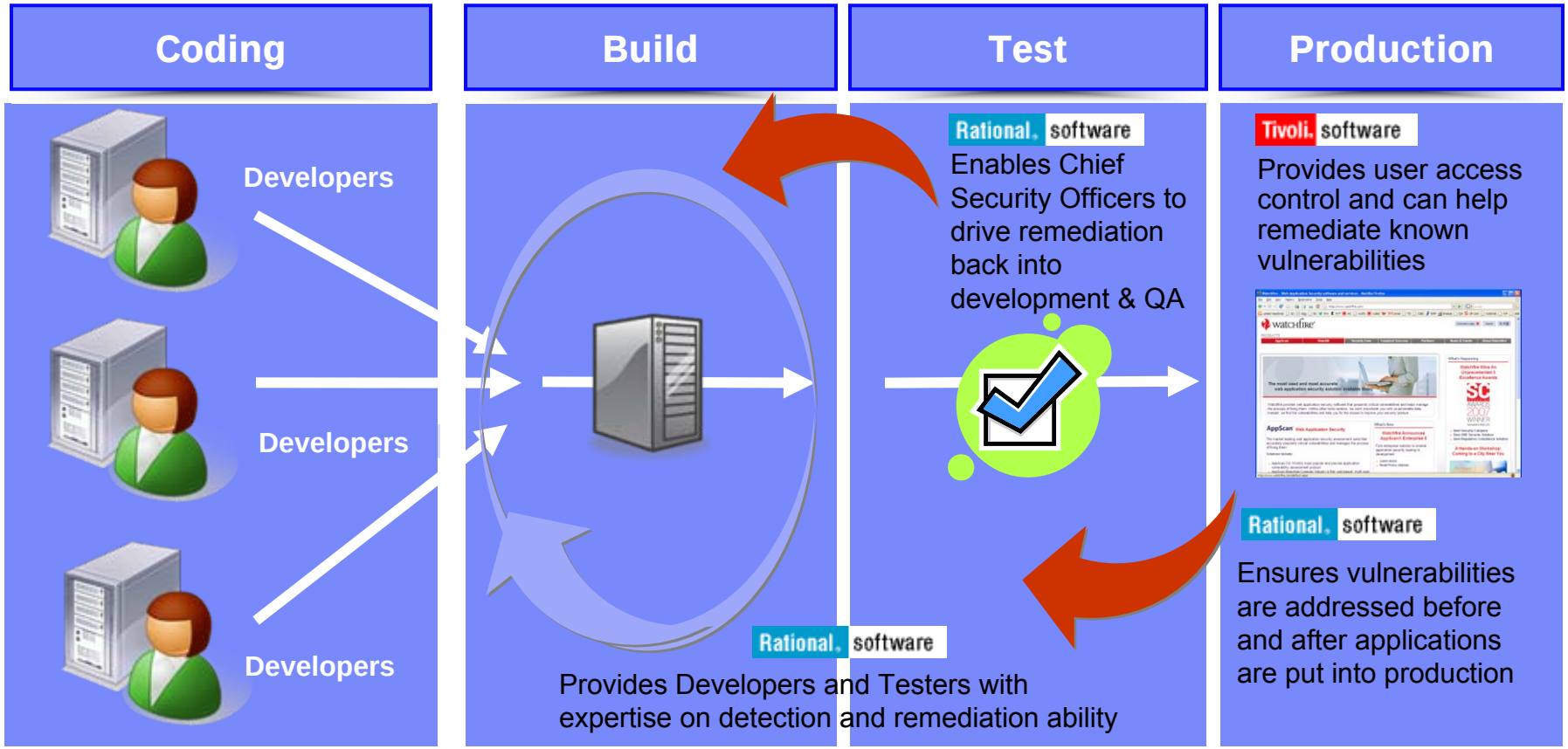
Reduces the need for scarce, RACF-trained expertise through a Microsoft Windows–based GUI for RACF administration

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.

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

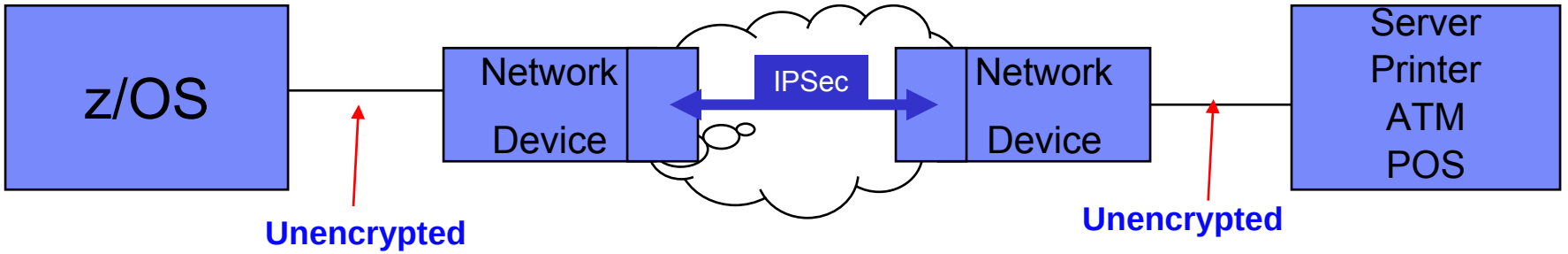


AppScan tests the application and RACF/Tivoli Access Manager secures access to them

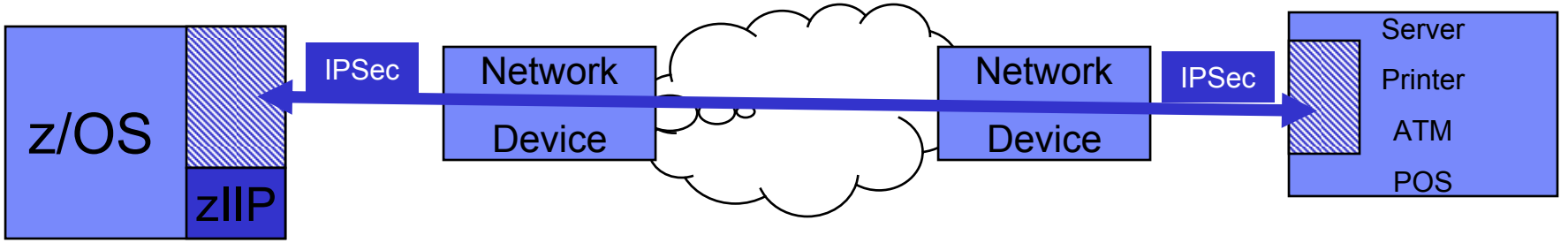
End-to-end network encryption

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

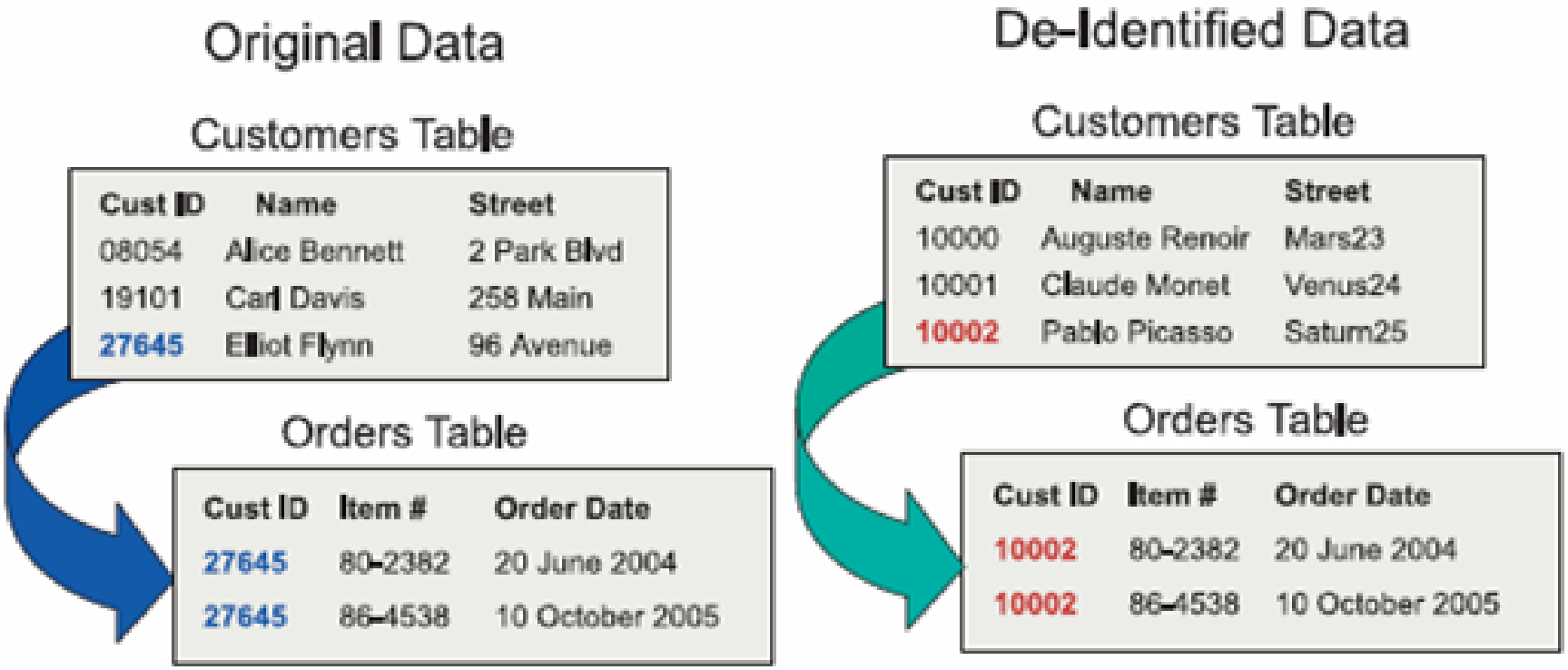
Database Capabilities

- 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**

Questions