Security and Compliance Considerations – Value of the Mainframe

Jim Porell

IBM Distinguished Engineer

System z Software

Mainframe Headlines

“IBM Touts Security of New Mainframe”

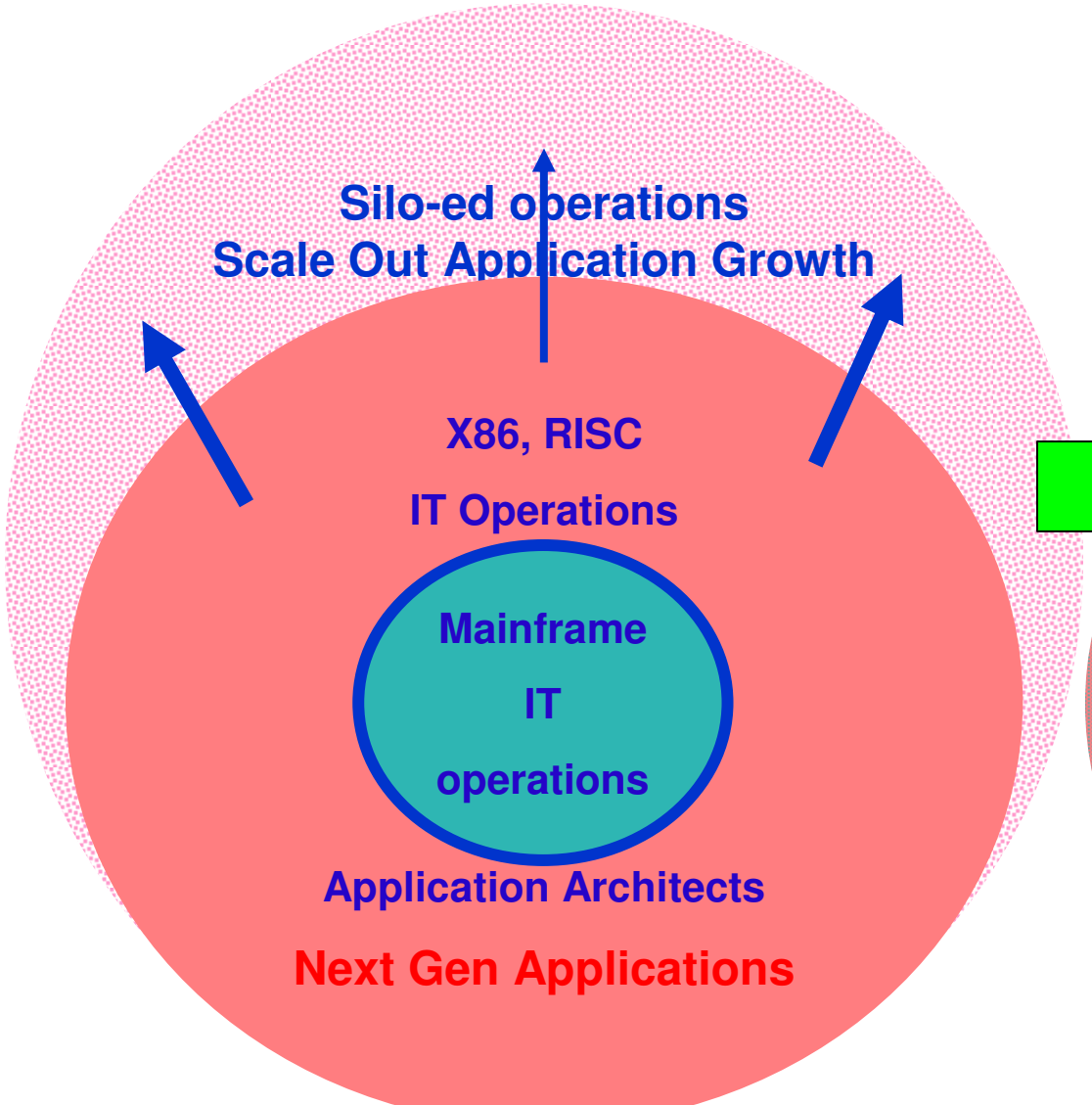
“IBM has done a remarkable job of renewing the mainframe”

“IBM announces mainframe virtual-tape offering ”

“the mainframe is heading towards a much larger potential market”

“IBM offers new mainframe software”

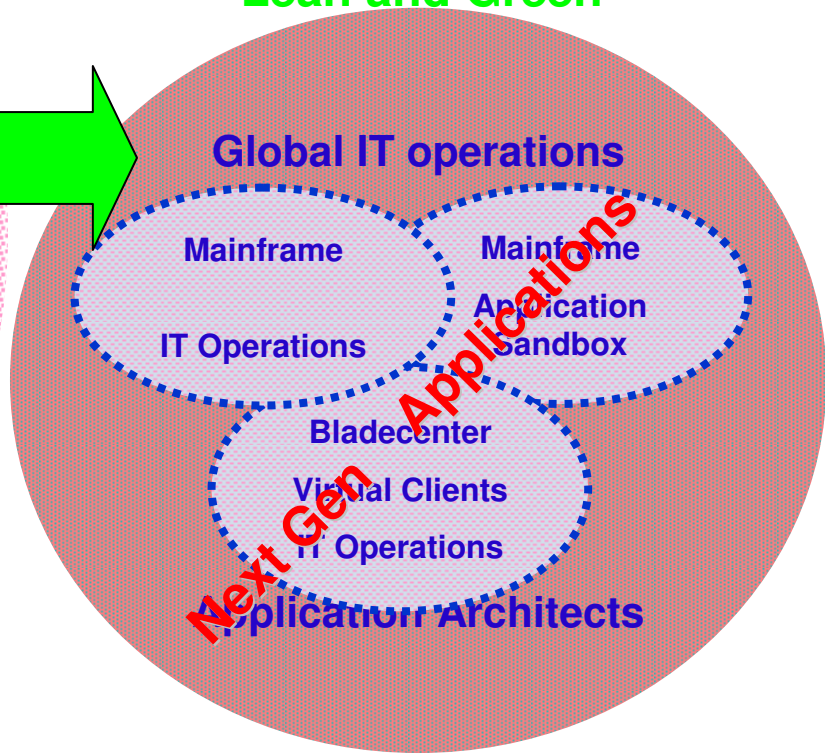
IT Management Trends are changing



Global Business Responsibilities

- Governance
- Risk and Compliance
- Business Continuity
- Privacy
- Agility

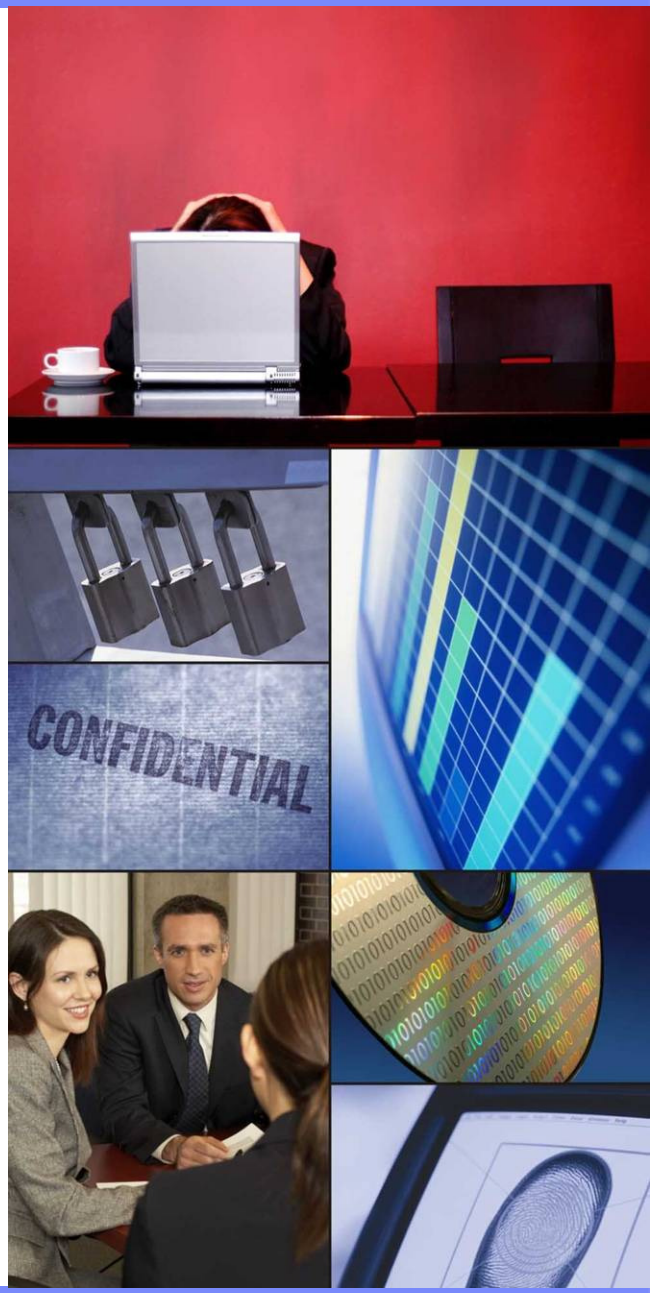
Lean and Green



IT security challenges

Need to maintain business innovation and growth in the face of risks

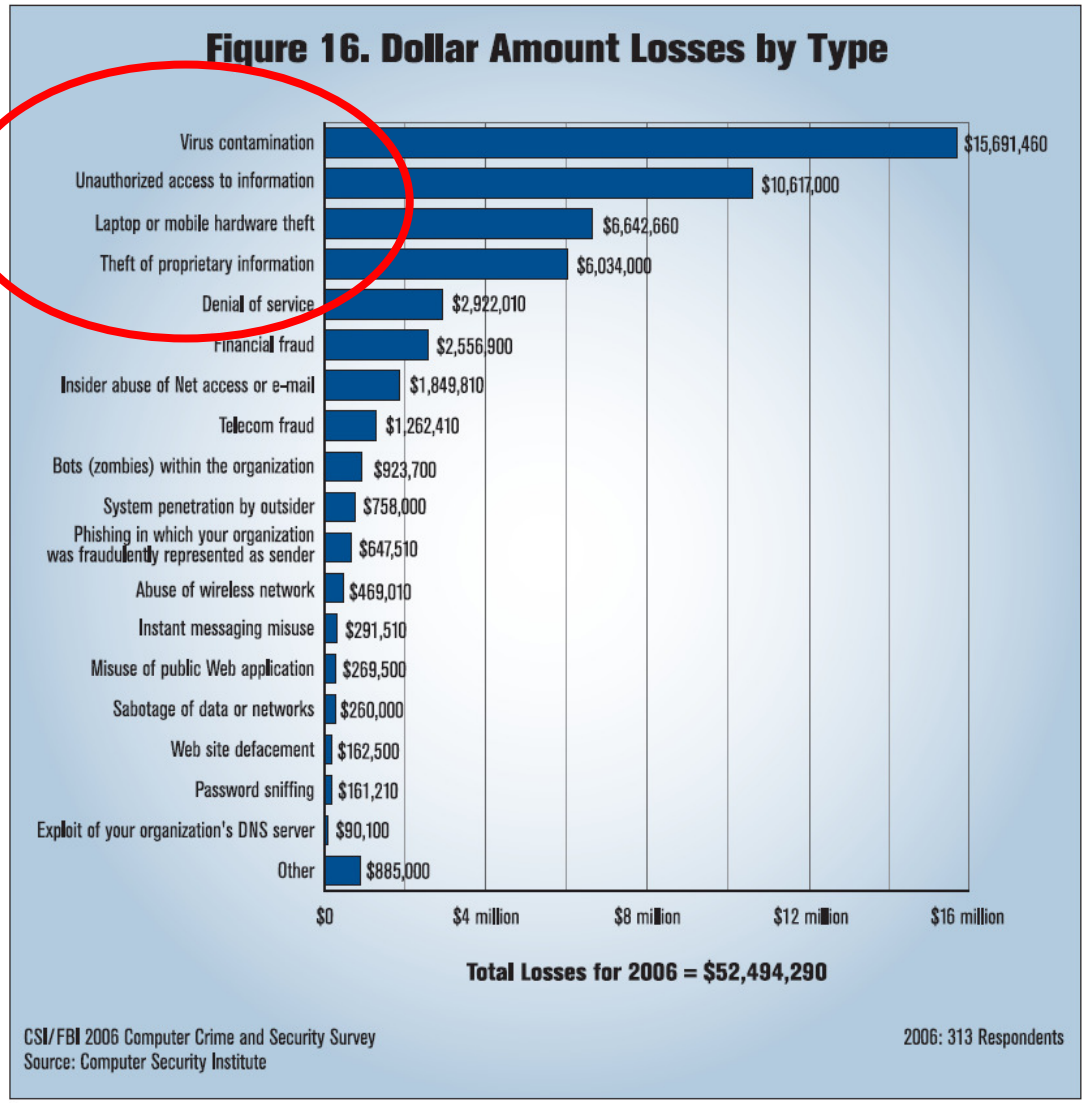
- **Increasing *complexity* of security issues in today's environment**
- ***Compliance* with regulations and audit requirements is difficult**
- ***Limiting* and *tracking access* to sensitive or private information and assets**
- **Establishing a *trusted relationship* with customers and partners**
- **Protecting against *security incursions* and *risks to confidential information***
- **Security issues are hurting the *bottom line!***



Cost of Security Incidents

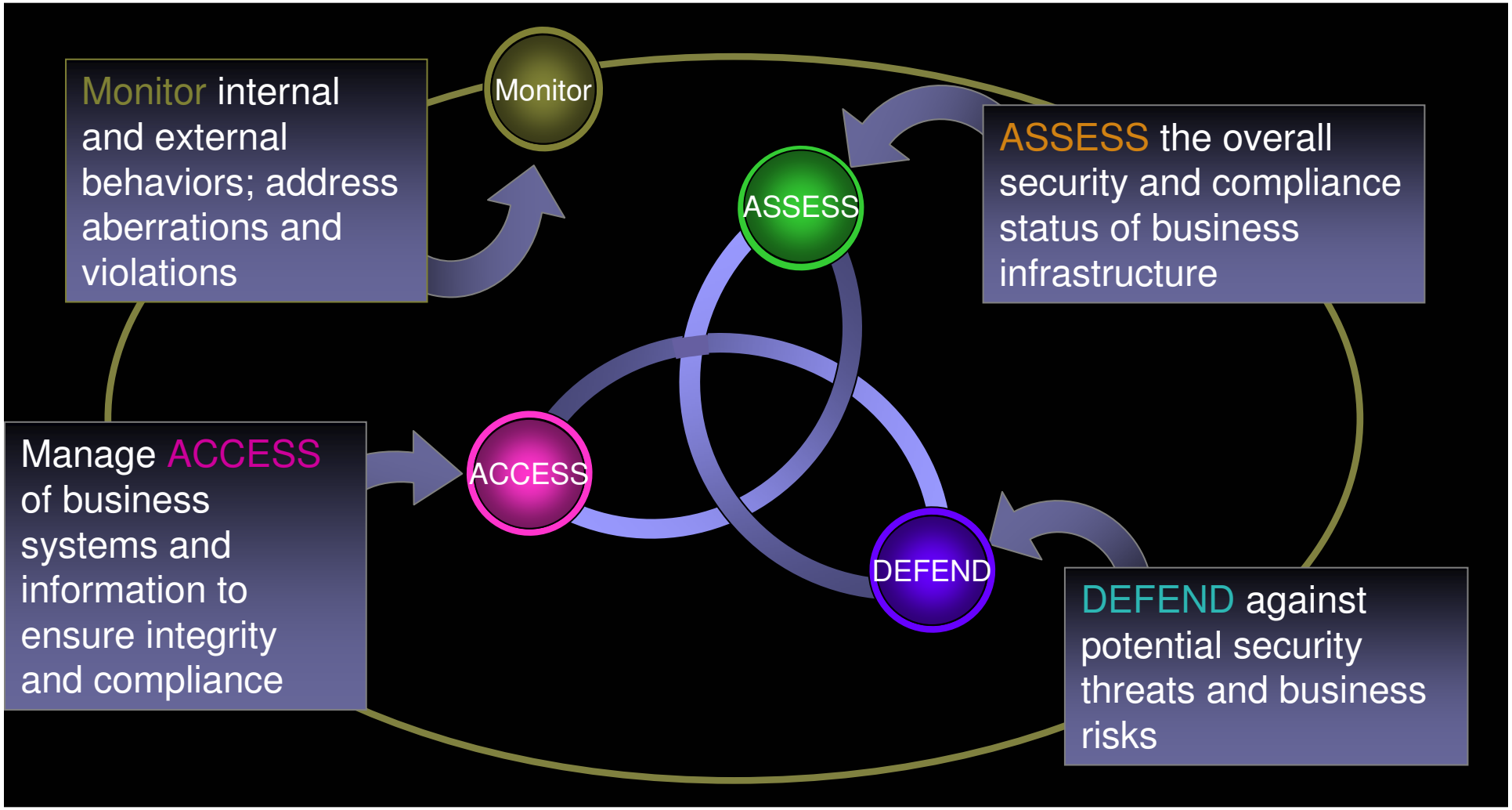
- **Computer Crime Survey indicates virus attacks still as the source of the greatest financial losses implying a need for a trusted platform**
- **Unauthorized access to information is second ranked, implying a need for better data protection.**
- Loss from unauthorized access to information:
  - **Was 303,234 in 2005**
  - **Is $10,617,000 in 2006**
- Loss from theft of proprietary information
  - **Was $355,552 in 2005**
  - **Is 6,034,000 in 2006.**

System z can address 4 out of the top 5 incidents (not laptop theft)



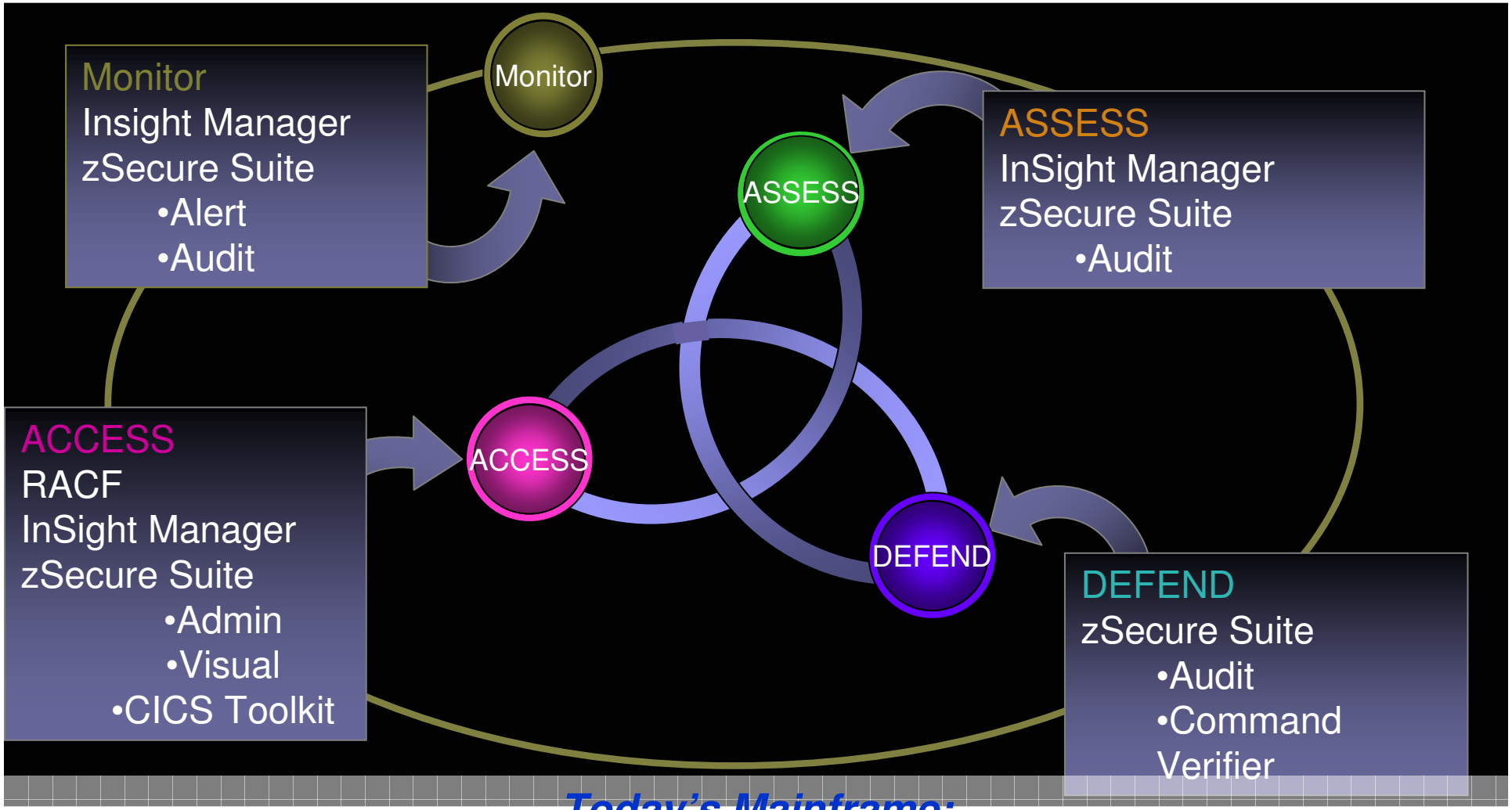
IBM's security management vision and strategy:

Preemptive, comprehensive security and compliance offerings



IBM's security management vision and strategy:

Preemptive, comprehensive security and compliance offerings



Today's Mainframe:

The power of industry-leading security, the simplicity of centralized management

IBM System z Value

Security

ID/Threat Management

EAL5

Encryption

Economics

New Entry Point

Growth Businesses

New Workloads

Power Efficiency

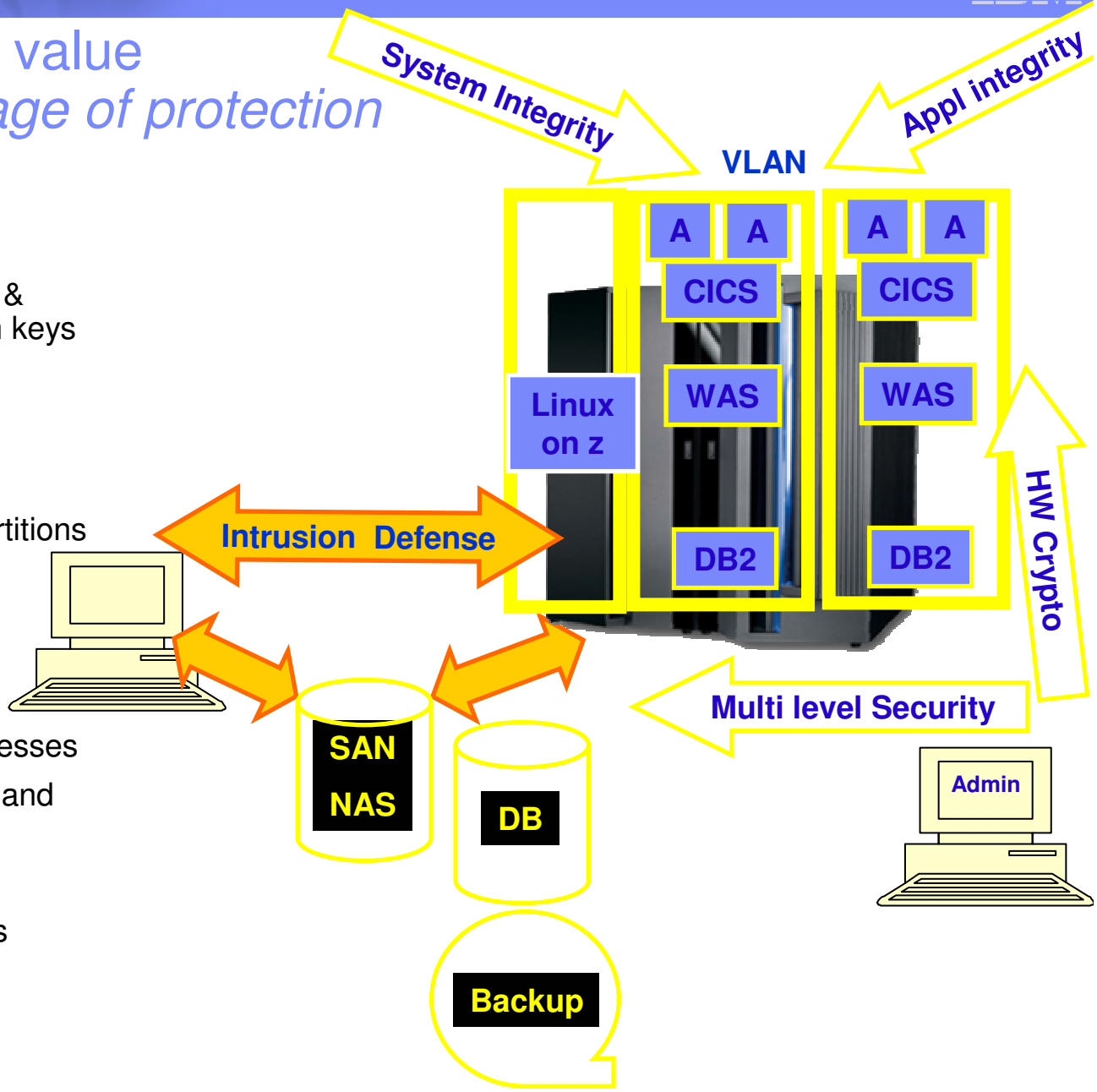
Power/Cooling Costs

Space

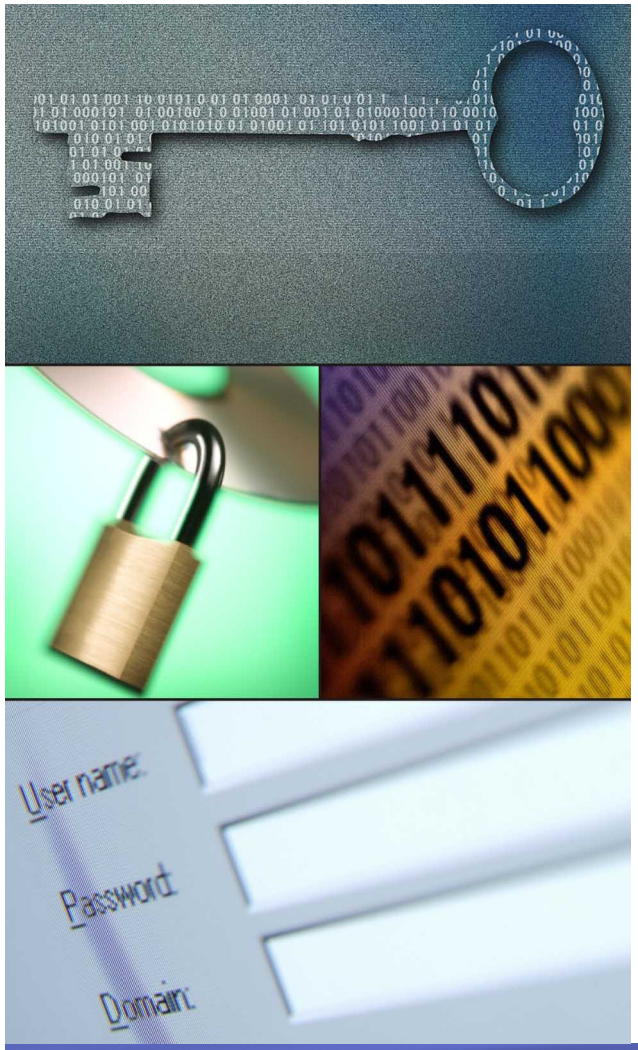
RFG Study

zSeries Architecture value
40 year heritage of protection

- **System & Application Integrity**
  - z/OS integrity statement
  - Inhibits trojan horses, worms & viruses via storage protection keys
  - Business Process Integration
  - Business Resilience
- **Compartmentalization of work**
  - Common Criteria certified partitions and guest isolation
  - Workload management
  - Virtual LANs reduce Security intrusion points
  - Middleware deployment processes
  - Row based security for DB2 and multi level security
- **Data Confidentiality**
  - Hardware encryption services
  - Encryption Key Management



System and application integrity by design



Integrity - the ability of the system to protect itself against unauthorized user or program access

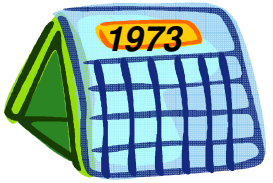
Workload isolation

Memory protection

z/OS (MVS™) and z/VM Integrity Statement

- IBM will **accept as Severity 1 any problems that describe exposures to the System Integrity**
- A lapse in integrity would allow unauthorized users to circumvent protection mechanisms

Since…



System z security advances

- **Transforming the economics of network and data protection:**
  - Enhancement to System z end-to-end network encryption with NEW IPSec use of zIIP specialty engine
  - Lower entry cost of secure-key encryption with NEW single port Crypto Express2 card for System z9 Business Class
  - z/OS, z/VSE and z/VM support planned for NEW low-end 3400 Tape Library featuring encrypting drives
- **Extending mainframe security for Linux**
  - NEW support for secure-key encryption with Crypto Express2
  - Multilevel Security support with NEW RedHat support for Security Enhanced Linux for System z (SELinux)
  - Stonegate solution for leveraging Linux as network DMZ
- **Giving you tools to help you meet regulatory reporting needs with confidence***
  - InSight and zSecure product suites from Consul – an IBM company
  - NEW DB2 9 and tools to improve security management, data encryption and auditing

*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.

System z Deployment Considerations

- **Supports Open Programming models**
  - Web services, Java, C/C++ - in both Linux for z and z/OS systems
- **Benefits of Scale Out environment in a Scale Up container**
  - Modularized to add server instances and functionality where and when needed – Software As a Service – On Demand
- **System z provides an open programming model with operational superiority to other platforms**
  - Applications can leverage best of x86/RISC worlds with mainframe to produce best Global IT Infrastructure TCO to customers.
- **System z becomes more of a Service Bureau for the enterprise, deploying Software as a Service**
  - Rethink your end to end Spreadsheets

Key Security Opportunities

- **Corporate Governance**
  - Audit, Reporting
- **Data Protection**
  - Cryptography – network, removable media, storage
  - Authentication
- **Virtualization – consolidation of workloads onto System z**
  - PR/SM LPAR and z/VM base
    - z/OS provides additional consolidation benefits
  - Compartmentalization of work
    - Labeled security with z/OS and Linux for z
- **Provisioning and Identity Management**

How PCI Compliance Works

- Consists of twelve basic requirements supported by more detailed sub requirements
- Based upon the size of the merchant or financial institution, there are audits that must be passed to achieve PCI certification
- The audits assess both implementation as well as policy and process
- Penalties and incentives can be substantial

*The **Payment Card Industry (PCI) Data Security Standard** is a result of a collaboration between Visa and MasterCard to create common industry security requirements. Other card companies operating in the U.S. have also endorsed the Standard within their respective programs. These 12 requirements are the foundation of Visa's CISP.*

PCI Data Security Standard

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect stored data
4. Encrypt transmission of cardholder data and sensitive information across 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 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

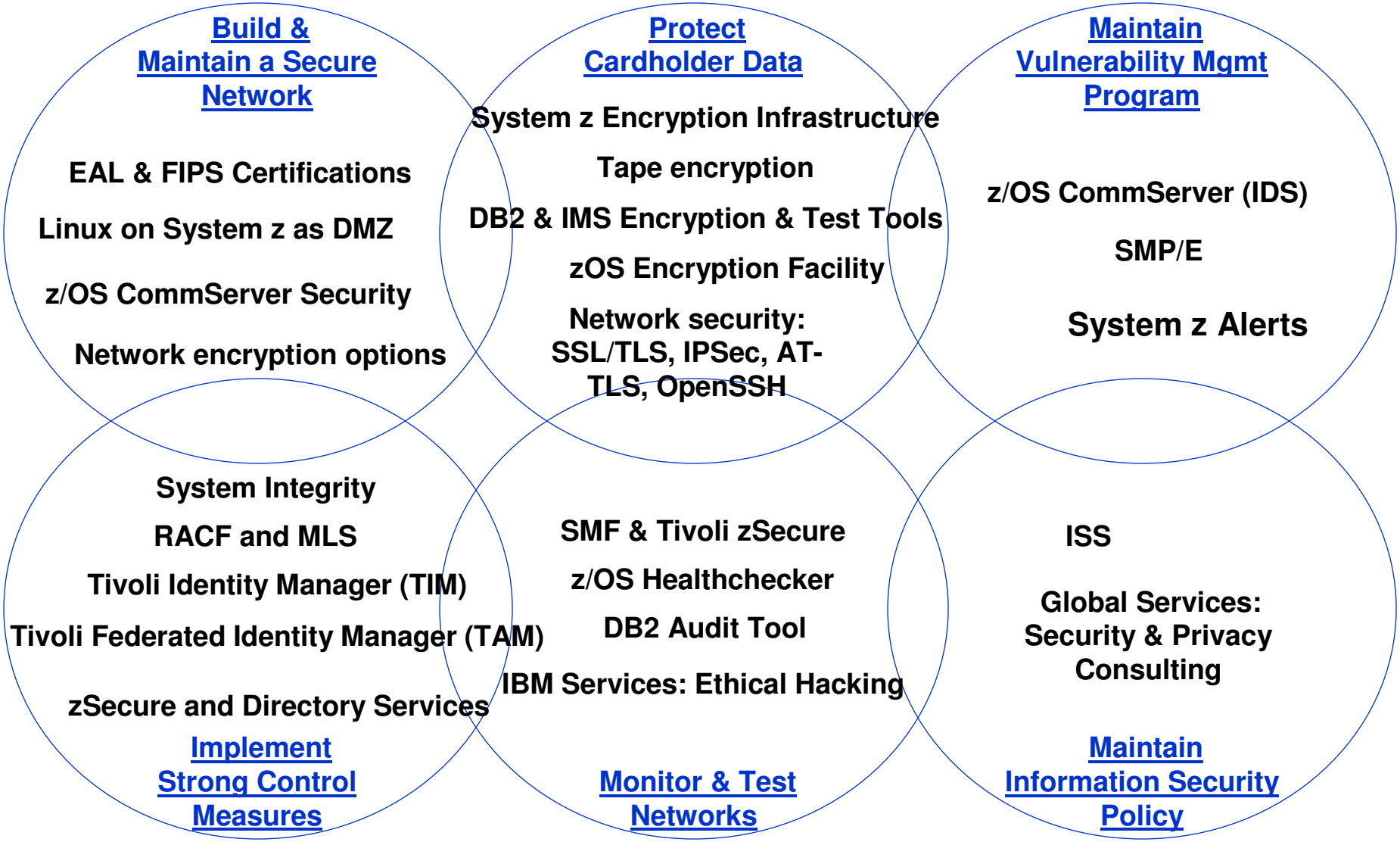
12. Maintain a policy that addresses information security

PCI DSS like most Security Initiatives is about

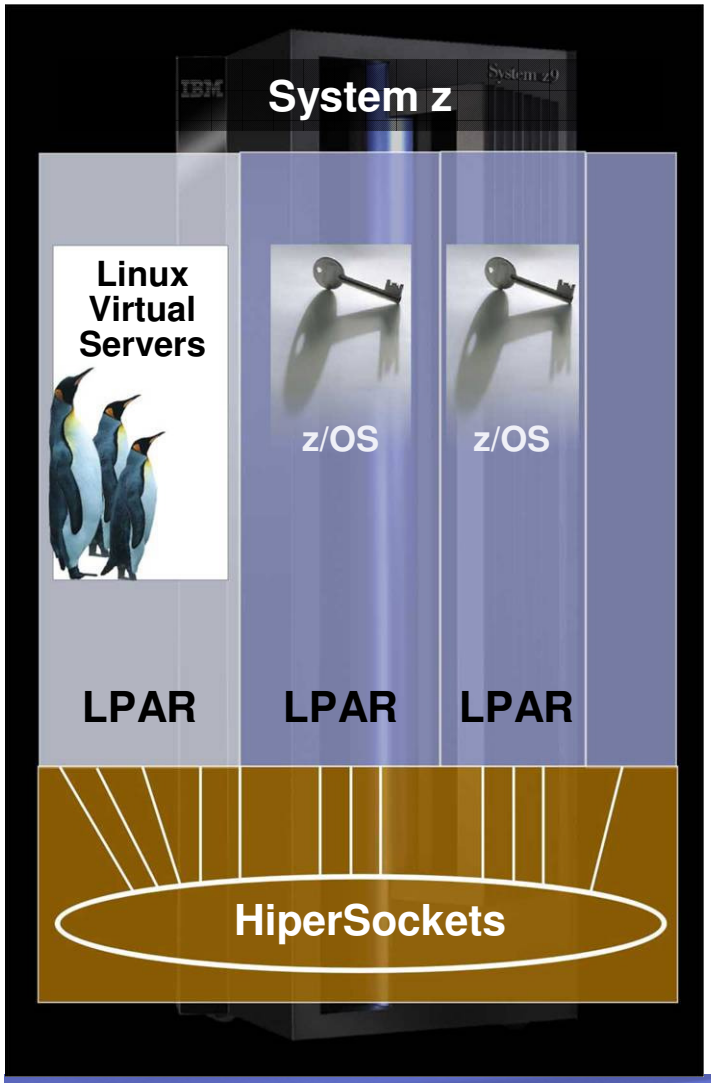
- People
- Process
- Technology

Leverage the mainframe policies and processes that have been developed over many years in your enterprise

System z features mapped to PCI six sections



Integrity through virtualization



- **Virtual servers on a single mainframe: Logical Partitions (LPAR)**
  - **Up to 60 isolated system images**
  - **Flexible dynamic provisioning of hardware resources**
  - **Highest Common Criteria certification – EAL5**
- **Virtual network in the server: HiperSockets**
  - **Provides an integrated TCP/IP network through system memory**
  - **Enables a "Data Center" inside a box with a mixture of z/OS and Linux images**
  - **Highly secure connection – no external network exposed**

IBM Consolidation Announcement Highlights

- ***IBM will consolidate thousands of servers onto approximately 30 System z mainframes***
- ***We expect substantial savings in multiple dimensions: energy, software and system support costs***
- ***Major proof point of IBM's 'Project Big Green' initiative***
- ***The consolidated environment will use 80% less energy***
- ***This transformation is enabled by the System z's sophisticated virtualization capability***

IBM'S PROJECT BIG GREEN SPURS GLOBAL SHIFT TO LINUX ON MAINFRAME

Plan to shrink 3,900 computer servers to about 30 mainframes targets 80 percent energy reduction over five years

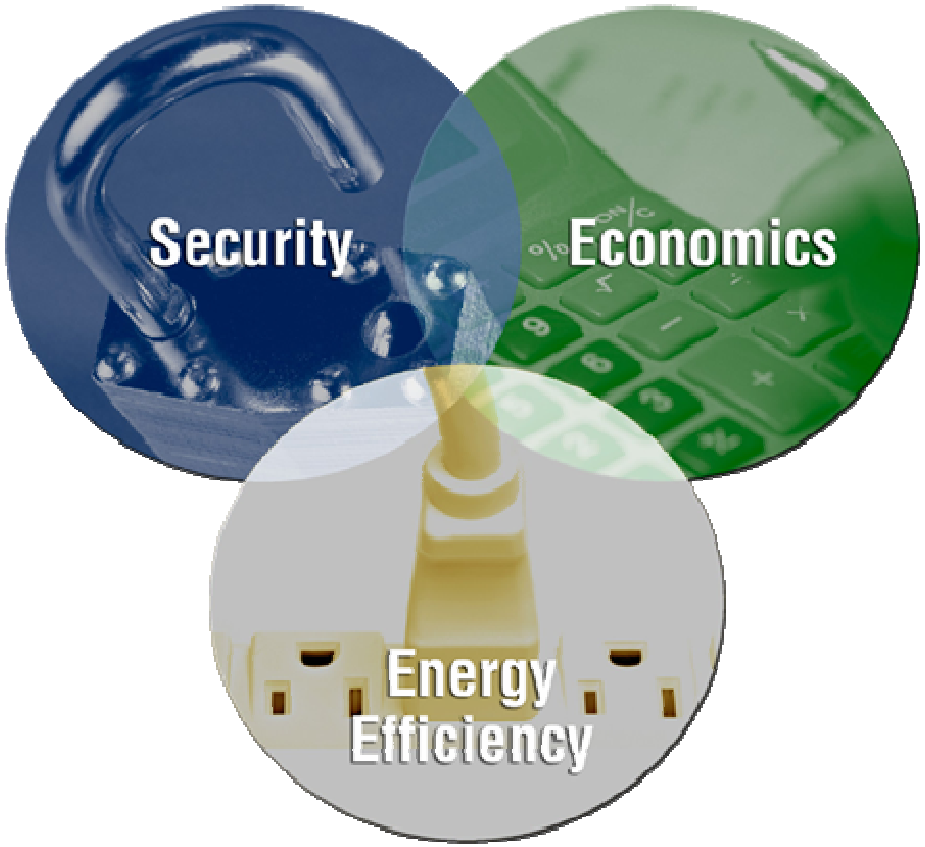
Optimized environment to increase business flexibility

ARMONK, NY, August 1, 2007 – In one of the most significant transformations of its worldwide data centers in a generation, IBM (NYSE: IBM) today announced that it will consolidate about 3,900 computer servers onto about 30 System z mainframes running the Linux operating system. The company anticipates that the new server environment will consume approximately 80 percent less energy than the current set up and expects significant savings over five years in energy, software and system support costs.

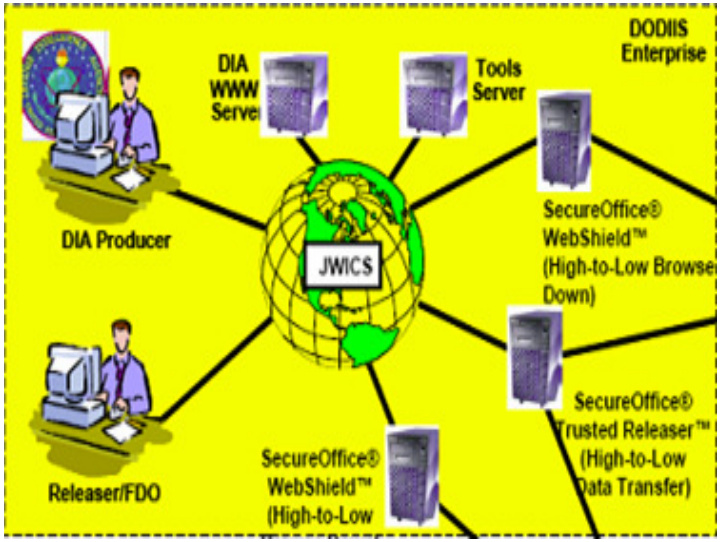
At the same time, the transformation will make IBM's IT infrastructure more flexible to evolving business needs. The initiative is part of Project Big Green, a broad commitment that IBM announced in May to sharply reduce data center energy consumption for IBM and its clients.

This is a cornerstone initiative in the IBM quality of service imperative

- **Leverages maturity of System z stack products for robust high availability**
- **Reduces complexity and increases stability**
- **Centralizes service level process management**
- **Potential for faster provisioning speed (months → days)**
- **Provides dynamic allocation of compute power**
  - **Capacity on demand; increase/reduce compute power**
- **Provides world class security**

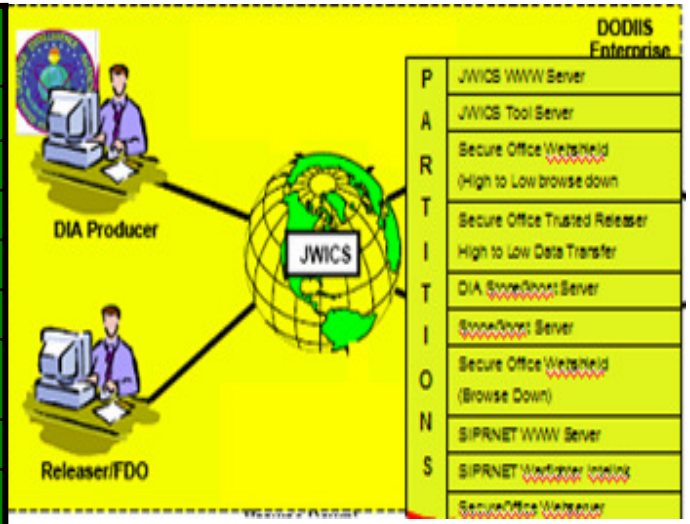


Secure Virtualization Changes Operational Model



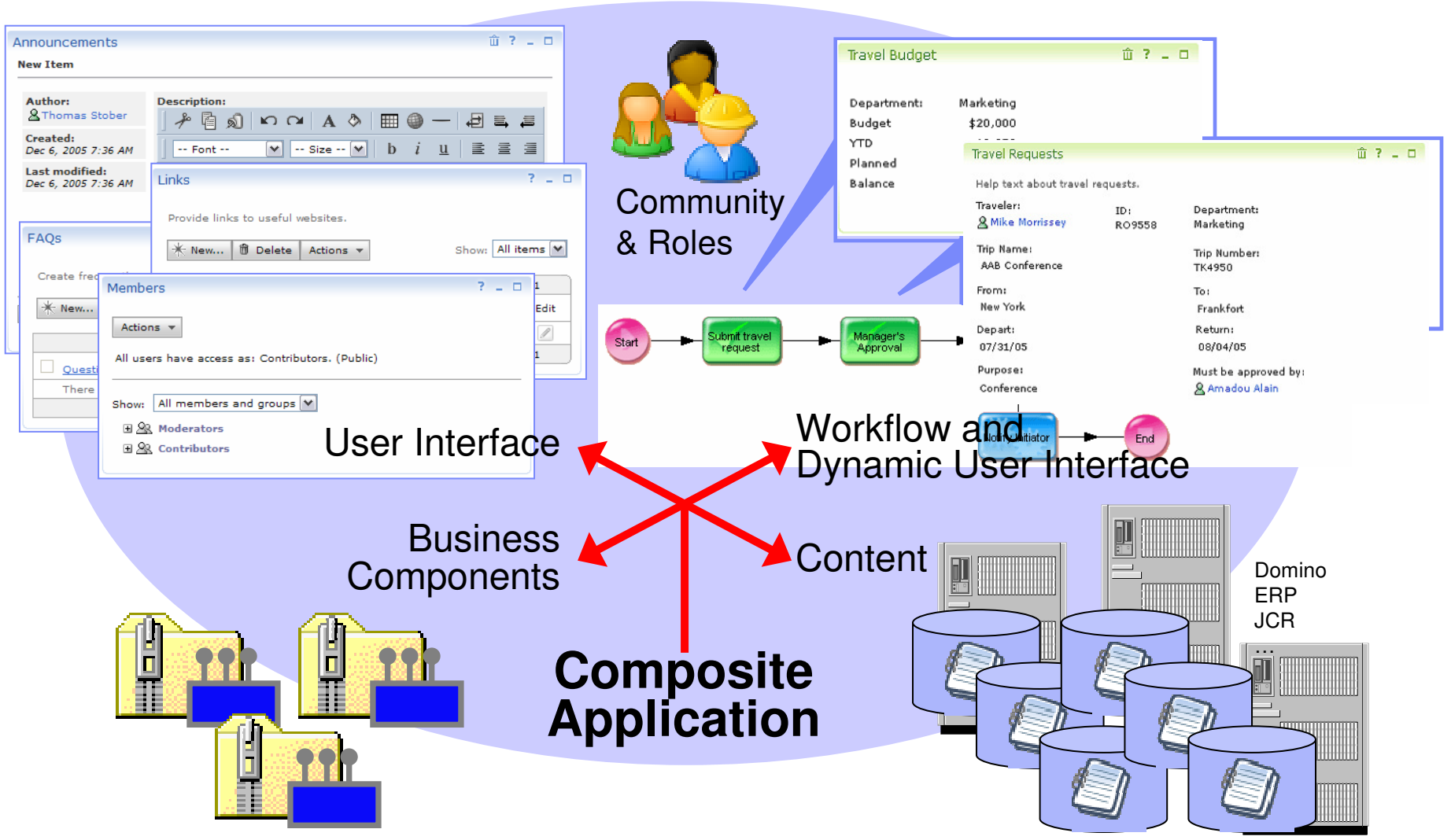
- **Cross Domain Database:**
  - Provide real time access to data avoid batch delays
  - collaboration across communities
- **Cross Domain Presentation Client**
  - Reduces desktop clutter
  - Reduce power consumption
  - Reduces leak potential with central mgt

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



Client Consolidation - CCON

Composite Applications



Network and data security
Expanded encryption capabilities on System z

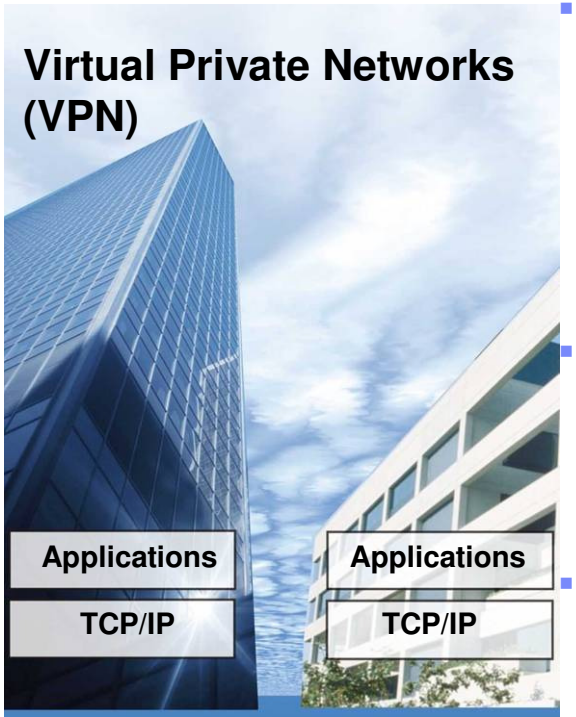
- **Network security**
  - Enhancement to end-to-end encryption with utilization of System z9 Integrated Information Processor (zIIP) specialty engine

- **Data security**
  - Lower entry cost for Crypto Express2 tamper-resistant encryption for IBM System z9™ Business Class (z9 BC)
  - Extending the scope of z/OS tape encryption key management to the TS7700 Virtualization Engine™ tape library and planned support for the new mid-range TS3400 tape library*
  - Encryption solutions for DB2 for z/OS
  - More flexible options for Encryption Facility for z/OS with OpenPGP support

- **Extending mainframe security for Linux**
  - Linux on System z™ support for Crypt oExpress2 secure-key encryption
  - Partner solution with Stonegate for leveraging Linux® as DMZ
  - Multilevel security with RedHat support for Security Enhanced Linux on System z

Network security – encryption over the Internet

Help secure access from the Internet

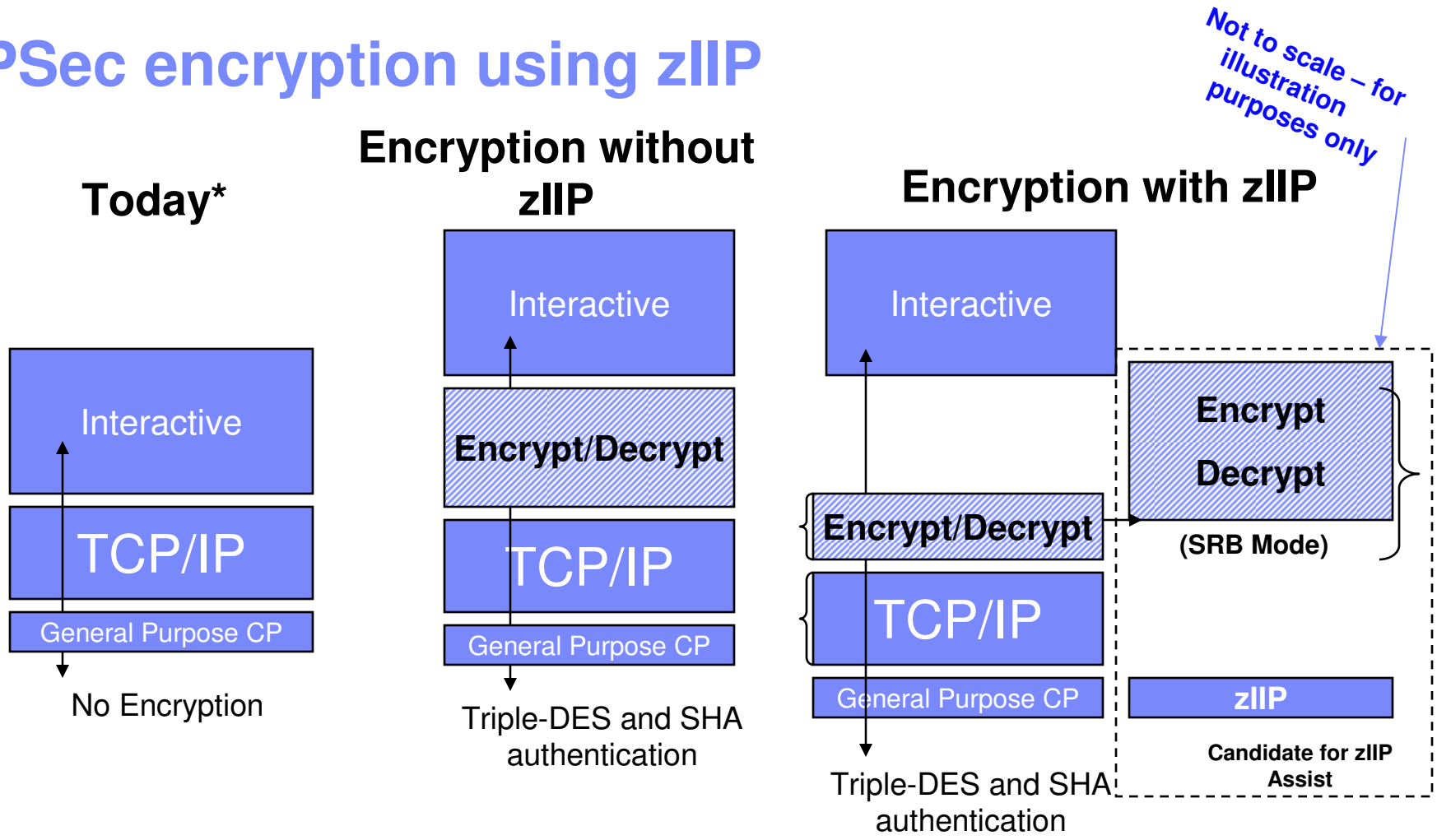


- **Application-layer encryption with SSL and TLS**
  - Encryption acceleration provided in each engine on System z server
    - Support for up to 6000 SSL handshakes per second*
  - Help reduce development complexity and costs with Application Transparent TLS (z/OS 1.7)
    - Define a TLS or SSL secured connection with no anticipated changes to existing applications
- **Network layer encryption with IPsec**
  - Allows secure tunnel between two locations (Virtual Private Network)
  - Improved scale and performance in z/OS 1.7
- **Simpler and consistent configuration of the above technologies**
  - *z/OS Network Security Configuration Assistant*

*** In a recent test using a System z9 with four CPs and both PCI-X adapters configured as accelerators the Crypto Express2 feature**

Mainframe uses latest technologies to help protect exchanges over the Internet

IPSec encryption using zIIP

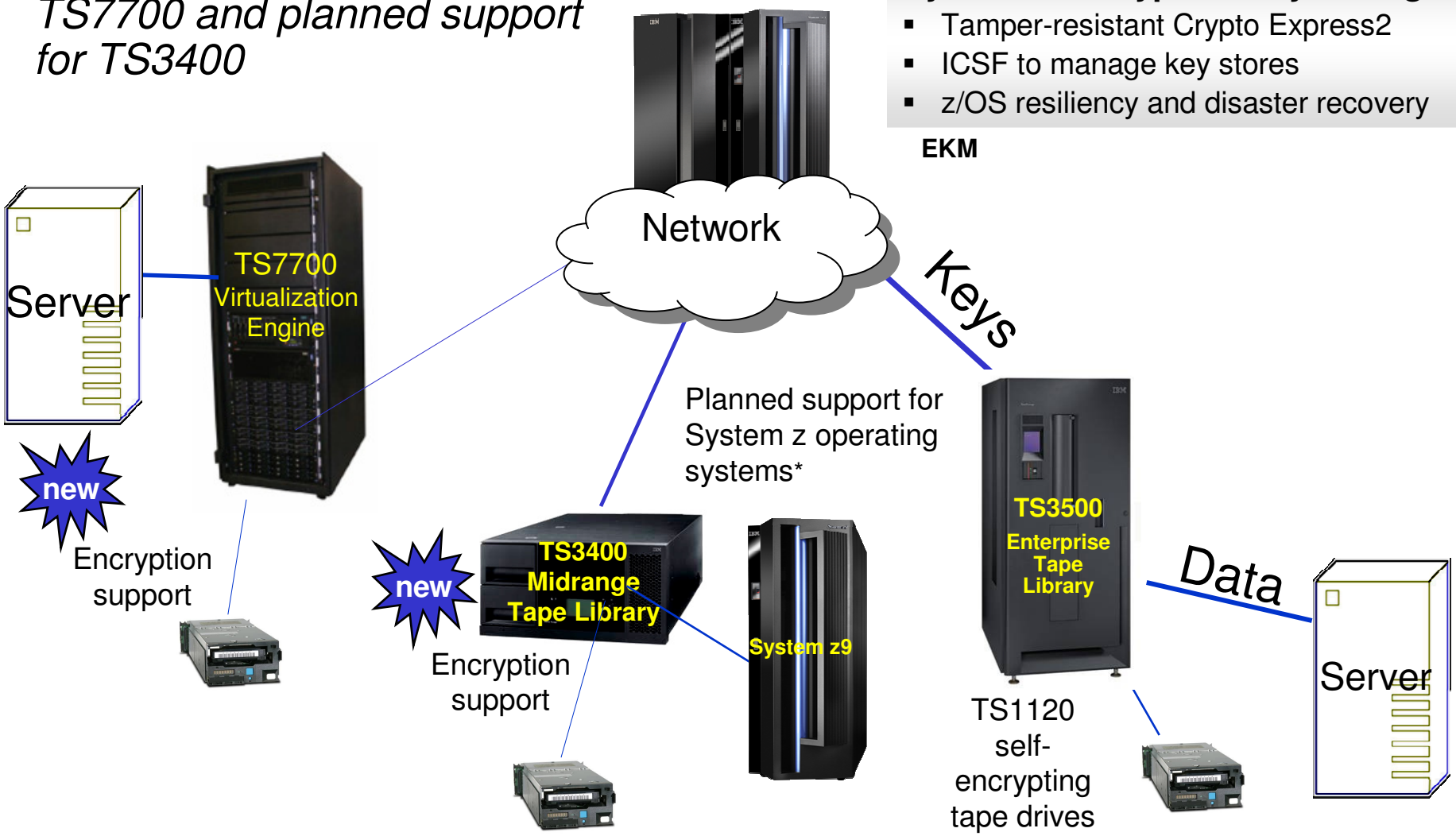


Function is enabled via a new TCP/IP configuration keyword when zIIP hardware in place and pre-req software

Enterprise tape encryption and key management

NEW: Encryption support for TS7700 and planned support for TS3400

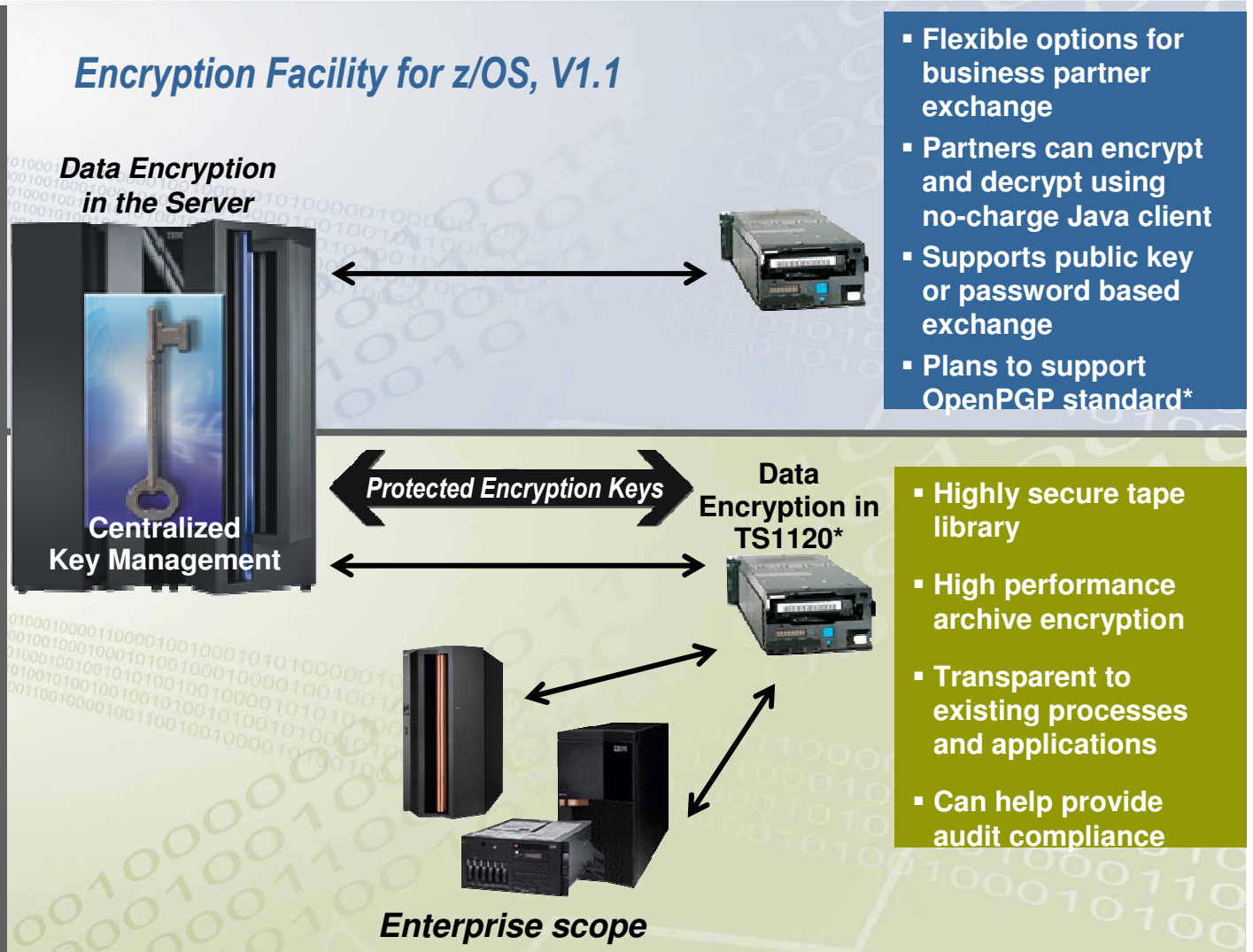
System z Encryption Key Manager
- Tamper-resistant Crypto Express2
- ICSF to manage key stores
- z/OS resiliency and disaster recovery



Tape Encryption with Key Management on System z

Why z/OS centralized key management?

- Can help to protect and manage keys
  - Highly secure and available key data store
  - Long term key management
  - Disaster recovery capabilities
- Single point of control
- Over a decade of production use



- Flexible options for business partner exchange
- Partners can encrypt and decrypt using no-charge Java client
- Supports public key or password based exchange
- Plans to support OpenPGP standard*

- Highly secure tape library
- High performance archive encryption
- Transparent to existing processes and applications
- Can help provide audit compliance

Protecting sensitive data with DB2 for z/OS

DB2 on z/OS encryption options:

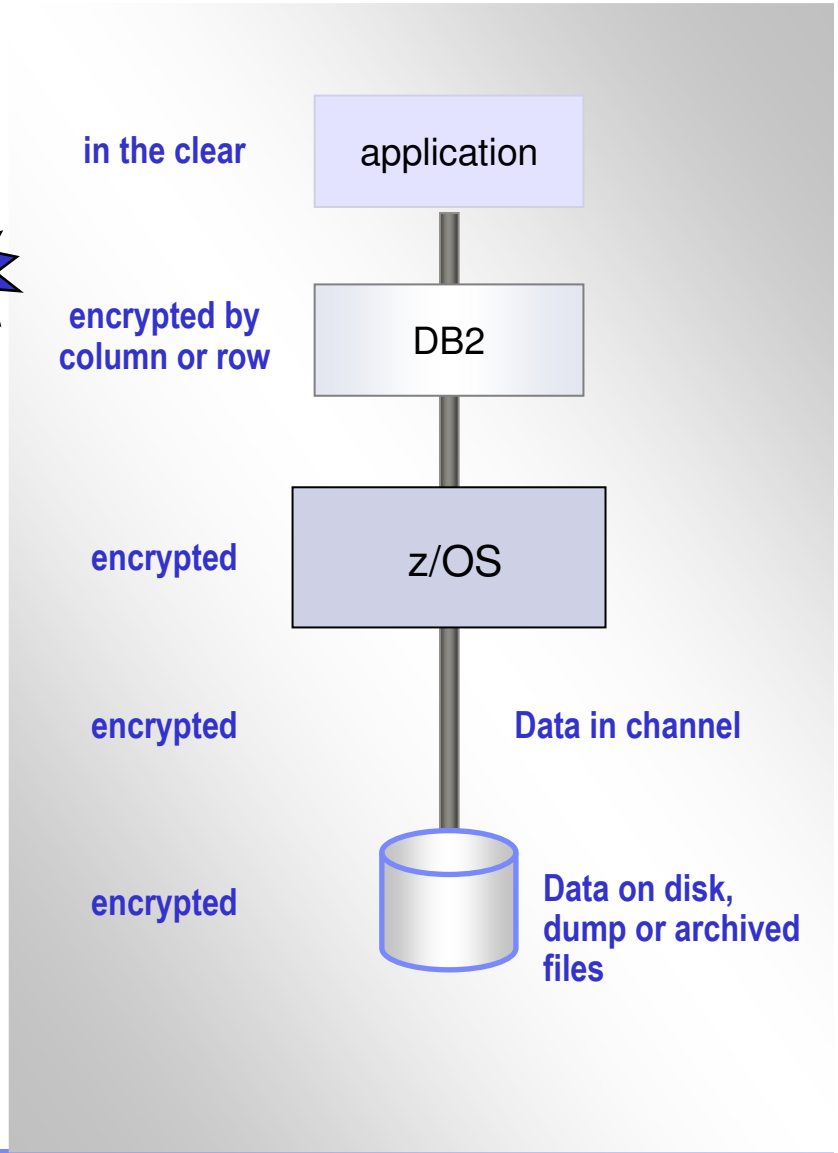
- **Encryption over the Internet**
  - **Encryption for DRDA® communications**
  - DB2 V9: SSL encryption for sending documents

new

- **Encryption in the database**
  - **Column level encryption**
    - Enabled by the application itself
  - **Row level encryption**
    - IBM Encryption Tool for DB2 and IMS™

Uses System z encryption acceleration and secure-key processing

- **Mask sensitive data used in test environments**
  - DB2 Test Database Generator



The power of Mainframe encryption
Helping to reduce risk

Customer objectives:

- **Only intended party is allowed to decrypt**
- **Availability of the keys and decryption services when you need them**

Mainframe encryption options

- **Privacy over the Internet to customers and partners**
- **Highly secure transmissions to Printers, POS, ATMs, Network Devices, Servers**
- **Data in DB2® for z/OS®**
- **Data transferred on tape to business partners**
- **Archived data**

Encryption acceleration

Secure-key processing

Centralized key management

Network security – z/OS intrusion prevention services

Detects events such as:
- Scans Attacks Flooding

Provides Defenses on z/OS
- Packet discard
- Limited # connections

Reports:
- Logging - Console
- Packet trace
- Notifications

A component of z/OS
Integrated in the IP stack

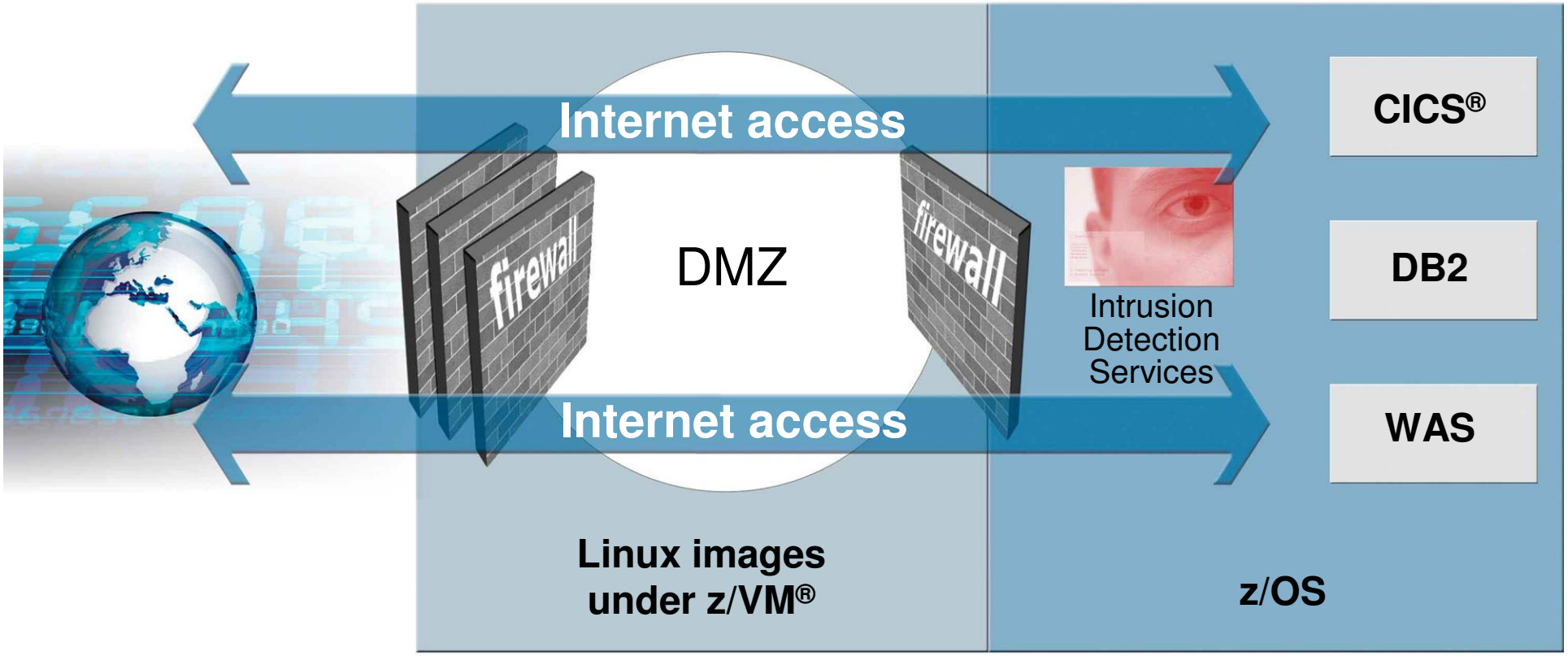
- Compliments network based IDS
- Enables further detection of attacks and application of defensive mechanisms
- Can be extended with Netview IDS

- Evaluates inbound IPsec encrypted data after decryption on the mainframe
- Evaluates many known attacks
- Can evaluate unknown attacks
- Detects problems in real-time
- Policy based
- z/OS 1.8:
  - No longer requires LDAP
  - Configuration assistant

Helps protect against network attacks
Can evaluate IPsec inbound data after decryption

Network security – perimeter defense
A DMZ on System z

- Consolidation to help ease of management
- Leverage the integrity of mainframe:
  - Logical Partitions with EAL5 certification and HiperSockets™
- *Stonegate™* for centralized firewall policy management and firewall workload balancing

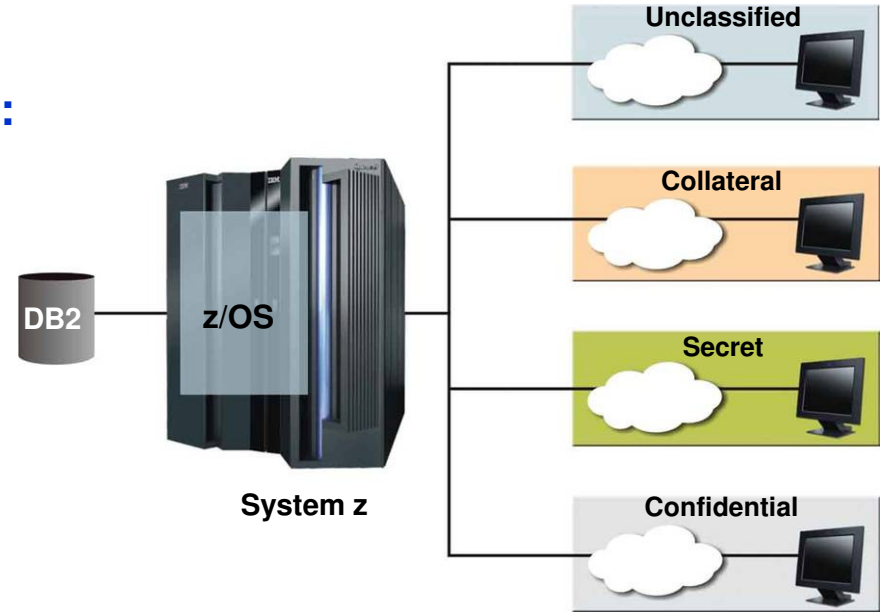


Multilevel security helps prevent declassifying of data

Multilevel Security (MLS) *helps prevent unauthorized users from accessing information at a classification level for which they are not authorized, or changing the classification of information they do have access to.*

MLS support with z/OS and DB2 is designed to:

- Protect confidentiality within a single database
- Security labels at DB2 row-level
- A common security manager, RACF®
- System z scale, availability and resiliency



new

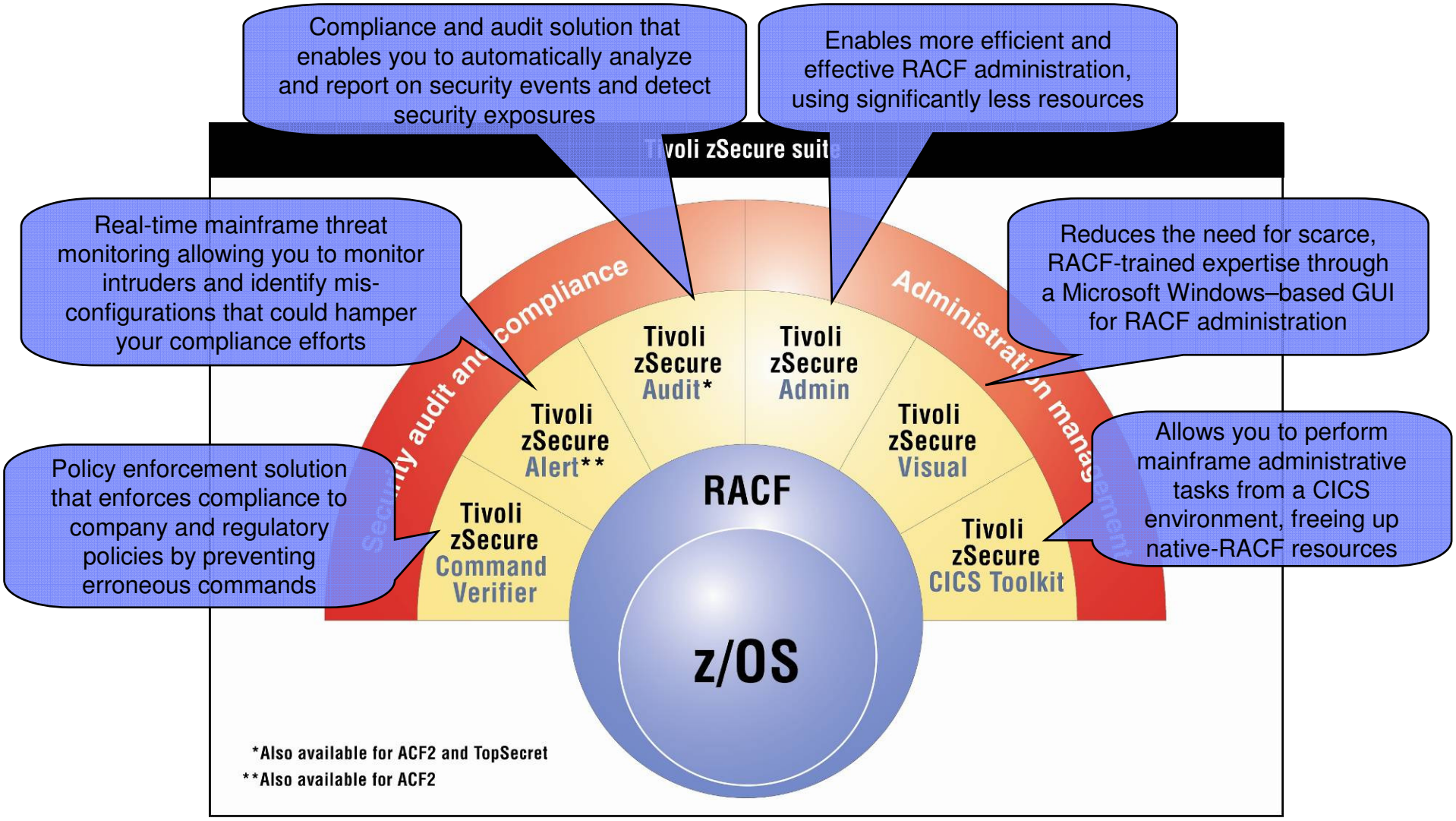
MLS support with Linux on System z

- RedHat support for Security Enhanced Linux for System z (SELinux)
- No integration with z/OS and DB2

"Red Hat and IBM have collaborated to integrate new security technologies that will help customers gain a competitive advantage in their respective industries. Security-Enhanced Linux is now built into Red Hat Enterprise Linux 5 to provide certified multilevel security capabilities to Linux for System z customers."

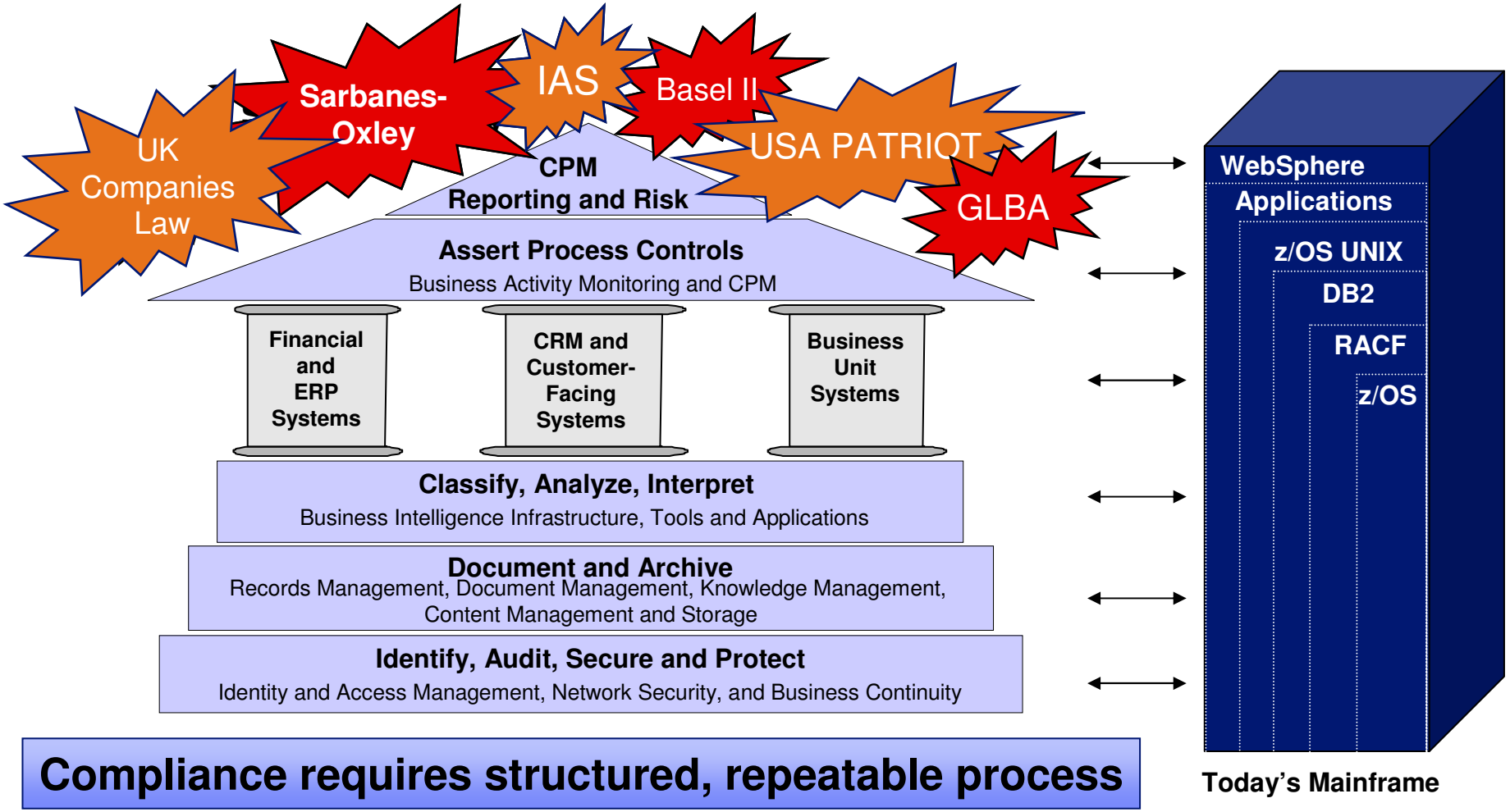
Paul Cormier, Executive Vice President of Engineering, Red Hat

Introducing the IBM Tivoli zSecure Suite



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

Security and Compliance Challenges – on the Mainframe

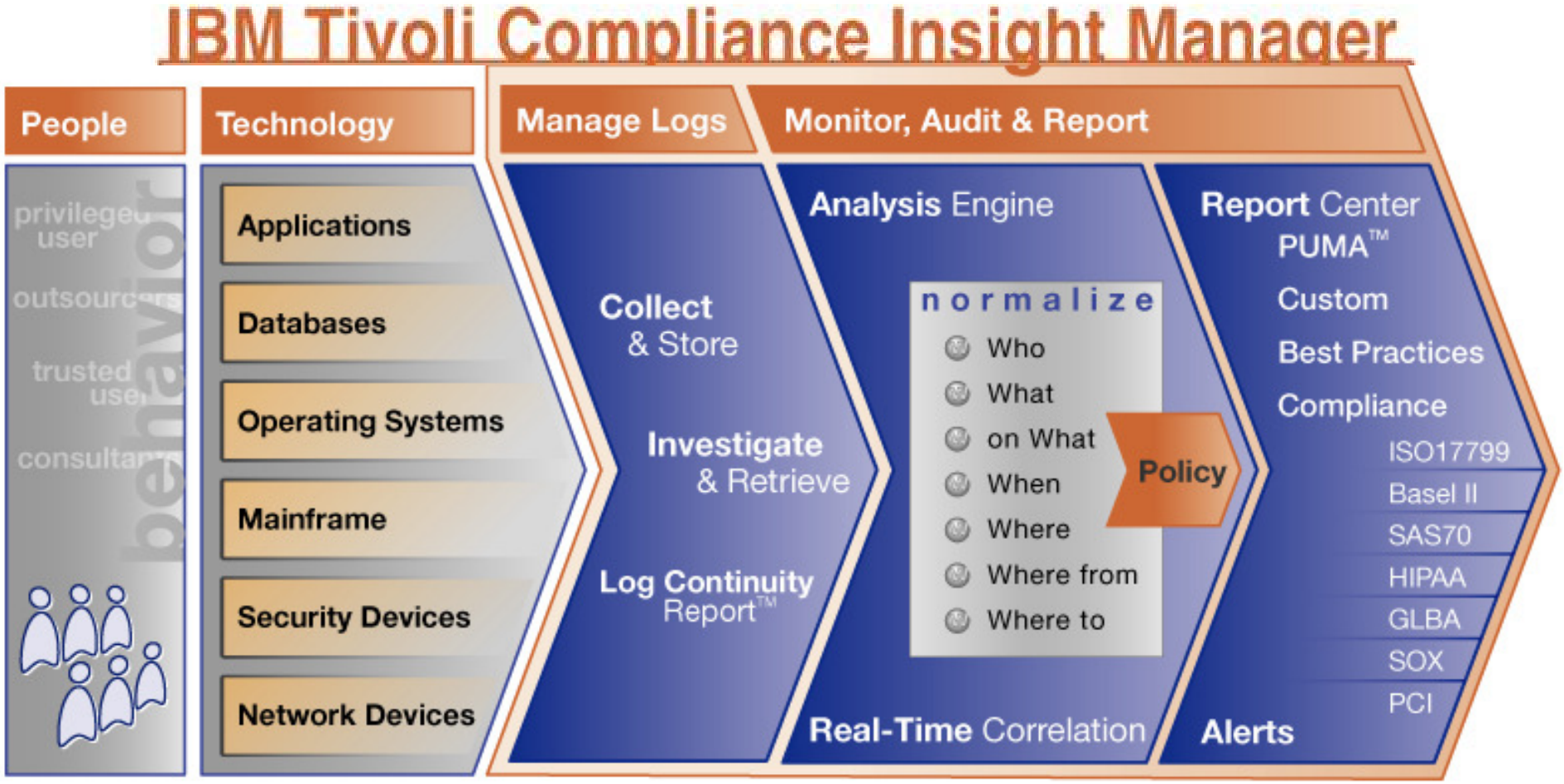


"Components of a Logical Compliance Architecture" Gartner, 2005

Compliance requires structured, repeatable process

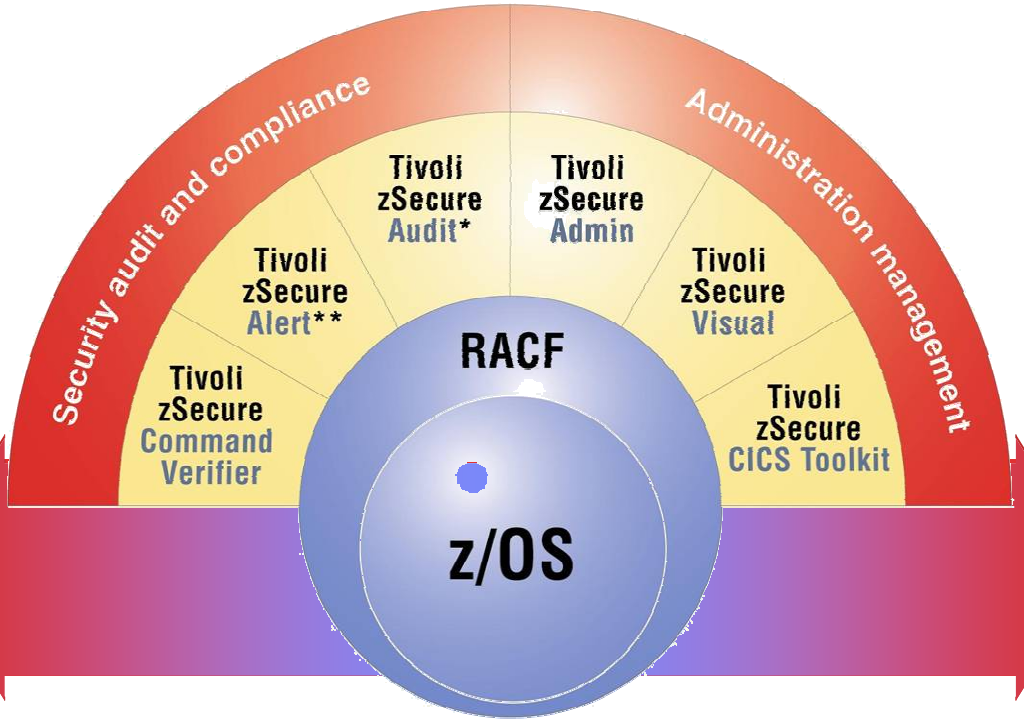
IBM Tivoli zSecure Compliance Insight Manager Enabler for z/OS

- **Integrate the Mainframe with TCIM Enterprise Compliance Dashboard**
- **W7 Patent Pending Analysis Engine**
- **PUMA (Privileged User Monitoring and Audit)**



A cornerstone for Tivoli's z/OS Security Strategy

IBM Tivoli zSecure Suite



* Also available for ACF2 and TopSecret

** Also available for ACF2

Enterprise Security Monitoring and Audit Reporting

Enterprise Identity and Access Management

Tivoli Compliance Insight Manager (TCIM)	Tivoli Security Operations Manager (TSOM)	Tivoli Identity Manager (TIM) for z/OS	Tivoli Federated Identity Manager for z/OS	Tivoli Directory Server for z/OS	Tivoli Directory Integrator (TDI) for z/OS

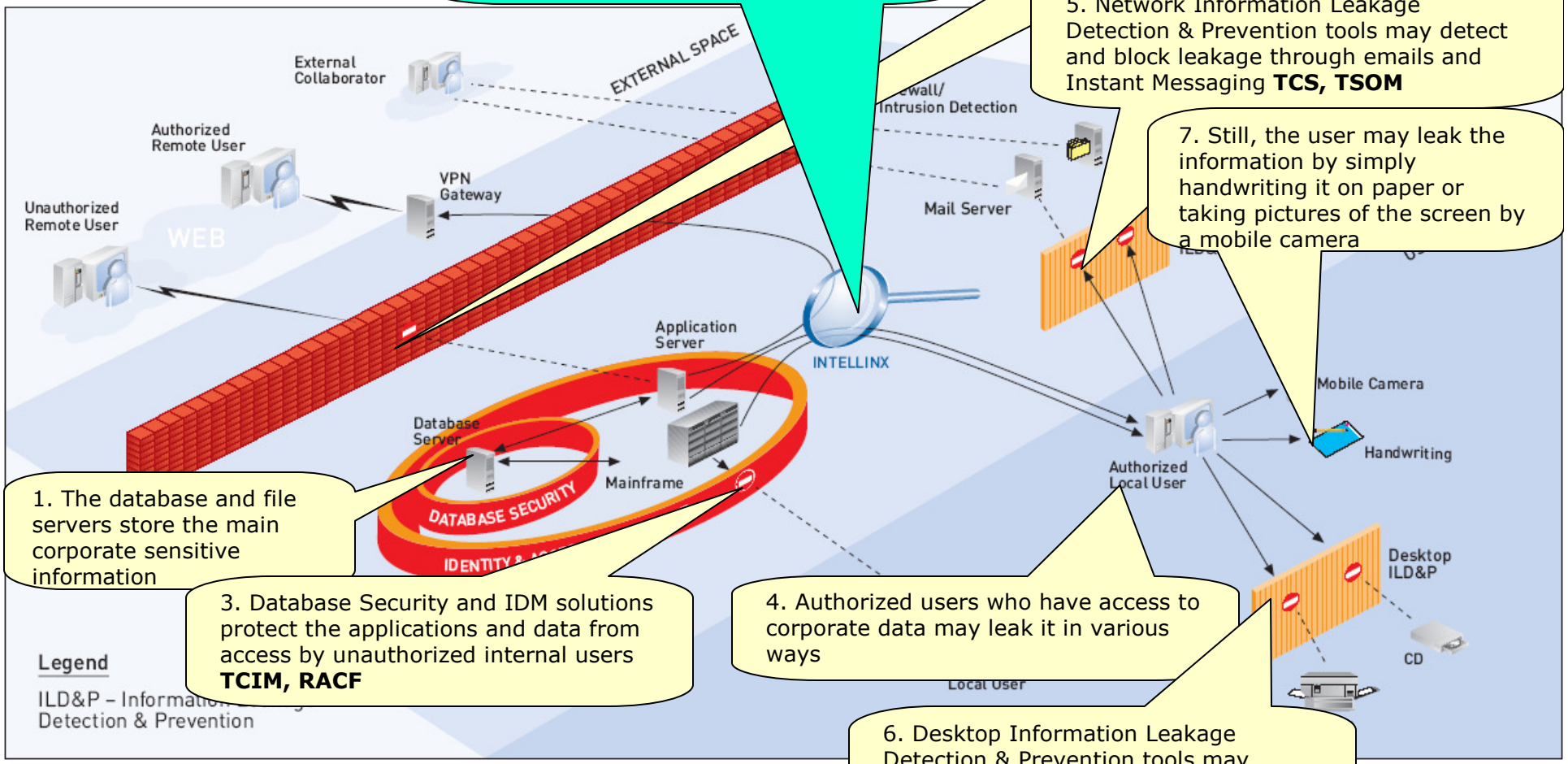
Insider Threat - Competitive Landscape

8. **Intellinx** provides protection at a different layer - the application layer. Discovery detects the sensitive information when it is retrieved by the user before it can be leaked. **Watchfire**

2. Firewalls and Intrusion Detection tools provide protection from access by unauthorized external users **ISS**

5. Network Information Leakage Detection & Prevention tools may detect and block leakage through emails and Instant Messaging **TCS, TSOM**

7. Still, the user may leak the information by simply handwriting it on paper or taking pictures of the screen by a mobile camera



1. The database and file servers store the main corporate sensitive information

3. Database Security and IDM solutions protect the applications and data from access by unauthorized internal users **TCIM, RACF**

4. Authorized users who have access to corporate data may leak it in various ways

6. Desktop Information Leakage Detection & Prevention tools may detect and block leakage through local printing and burning CDs / Flash USB cards **TCS, Thin/Hosted Clients**

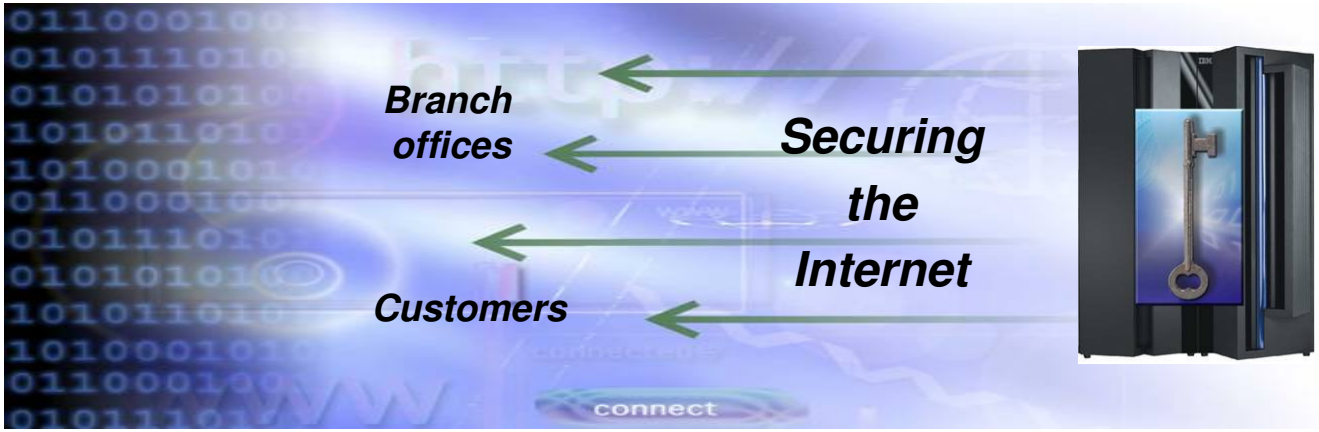
DB2 Regulatory Compliance Suite

Objective	Set of Tools
Use encryption to protect your vital information	***Encryption Tool for IMS and DB2* databases** – Supports both secure key and clear key encryption – Low overhead, high performance with System z9 Encryption features in ***DB2 for z/OS***
Generate test data while protecting your assets	***DB2 Test Database Generator*** – Protects sensitive data when needed in test environments – Preserves data relationships
Retaining data to comply with policies	***DB2 Data Archive Expert*** – Simplifies and automates archive of data for retention requirements
Analyze unauthorized usage of your data	***DB2 Audit Management Expert*** – Lets you determine who did what to what and when, for the DB2 environment

System z Security hub for the enterprise

Banco do Brasil

- **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**
  - **using the encryption solutions included in z/OS and their System z™ server**



BANCO DO BRASIL

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

Secure and Efficient "Smart Card" Solution at Banco Itaú Fights Fraud and Saves

- **Banco Itaú S.A. is one of the largest banks in Brazil**
  - **approximately 3,000 branches, 20,400 automated teller machines and 42,200 employees**
  - **15M checking accounts, 9M savings accounts, 6M credit cards**

- **Situation:**
  - **To meet efficiency objectives and ensure the security of its 12 million issued debit cards, Banco Itaú replaced its regular cards with security chip-enabled smart cards.**
  - **Need improved security so that new markets and customers can trust the bank while getting quick and easy access to their accounts**

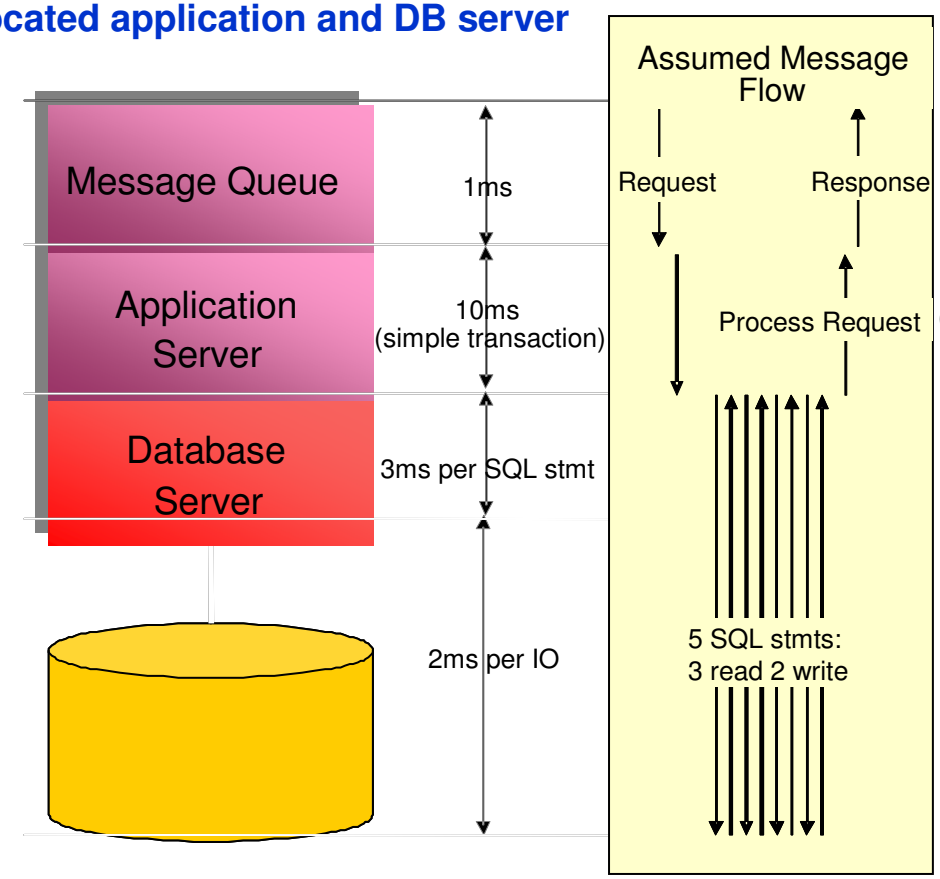
- **Problem:**
  - **Performance bottleneck with Thales e-Transactions security servers (which process "smart cards")**

- **Solution:**
  - **Leverage superior mainframe security, eliminate separate security server and migrate smart card solution to the mainframe**
    - **All core business systems run on mainframes**
    - **System z reliability and technical support also key factors in this decision**
    - **Better price performance**
  - **Install mainframe PCI Cryptographic Coprocessor cards (PCICC)**
    - **Encryption keys are generated and stored on PCICC cards and used for smart card authentication, blocking and password change**
    - **Use IBM z/OS V1.6 security APIs**

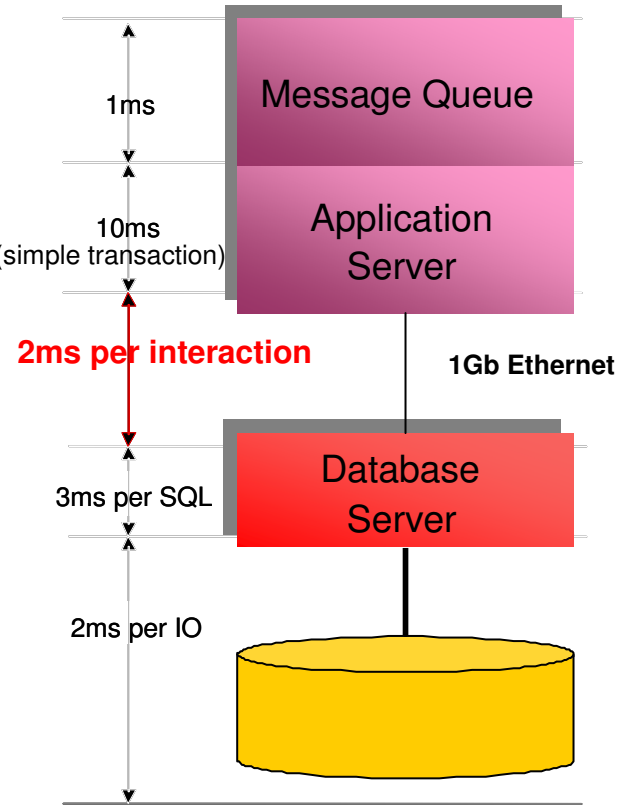
- ***Result:*** **Reduced fraud from stronger smart card security, reduced costs, PLUS increased stability, efficiency, and faster processing**

Proximity to data – online banking workload analysis

Co-located application and DB server



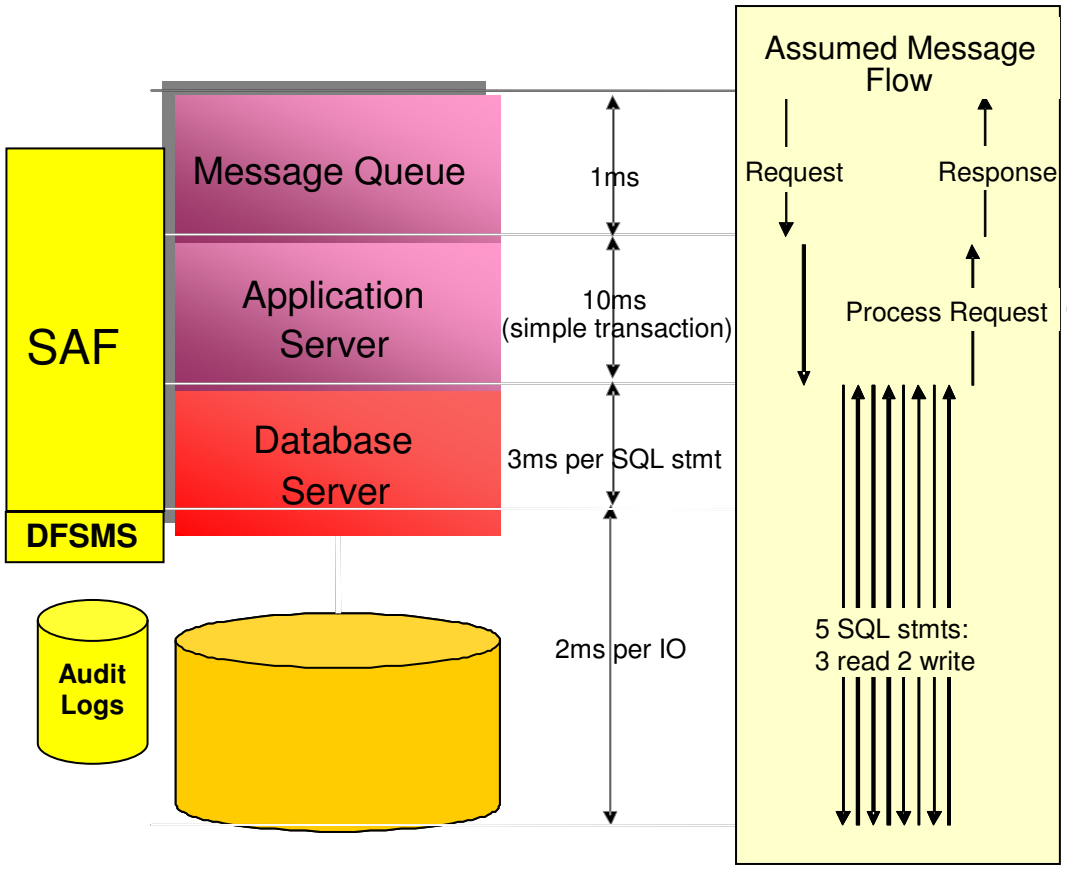
Distributed application and DB servers



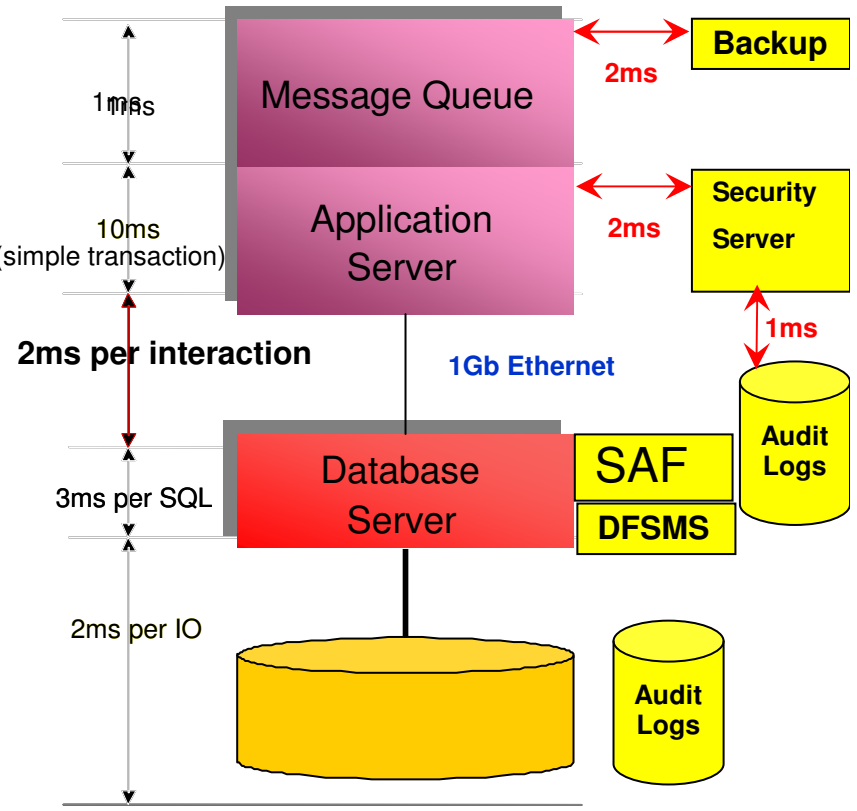
- **Evaluation of the application and data on multiple physical servers:**
  - Overall transaction throughput (at constant response time) would be degraded 33%, requiring more capacity than originally planned
  - A significant amount of memory was required to hold in-flight work, comprising 80% of each server's cost

Proximity to data – online banking workload analysis

Co-located application and DB server

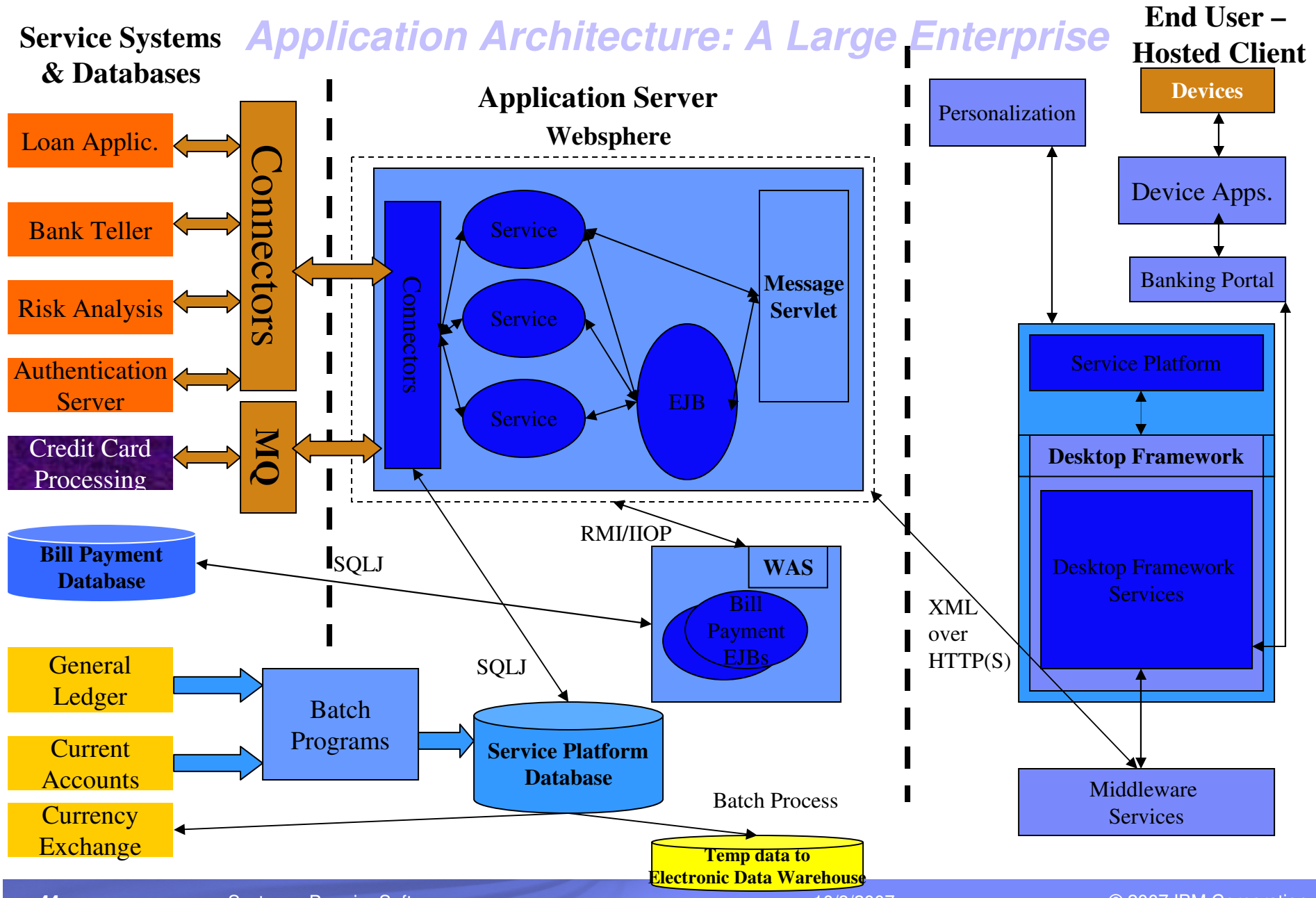


Distributed application and DB servers

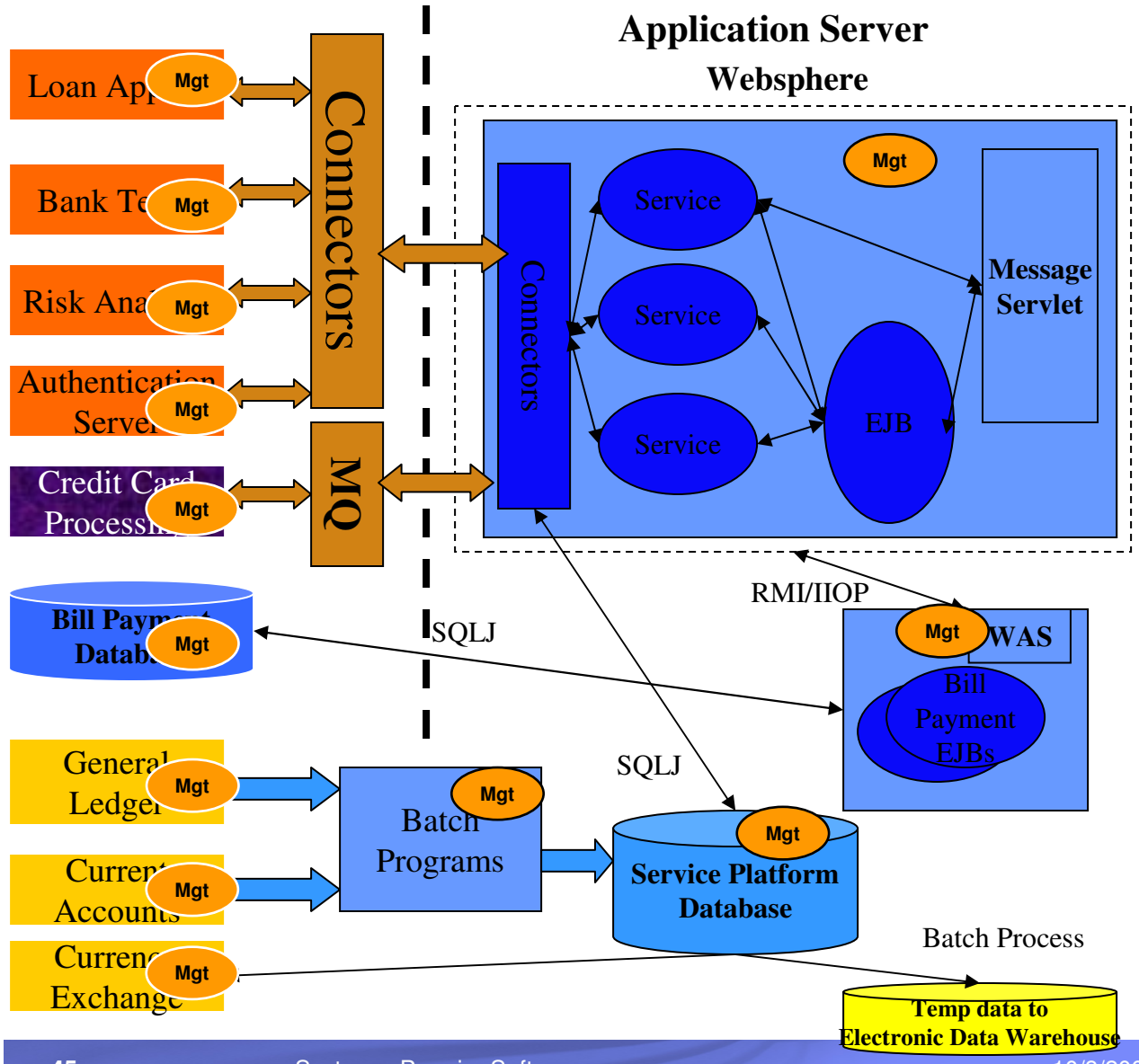


- **Prior chart might be best case scenario. Add "non-functional" requirements:**
  - Additional authentication flows – more interconnect and i/o required
  - Audit complexity may increase to correlate access to personally identifiable data
  - Business Resilience solutions may be more complex; Additional environmental costs
  - Storage management costs across the workflow

Application Architecture: A Large Enterprise



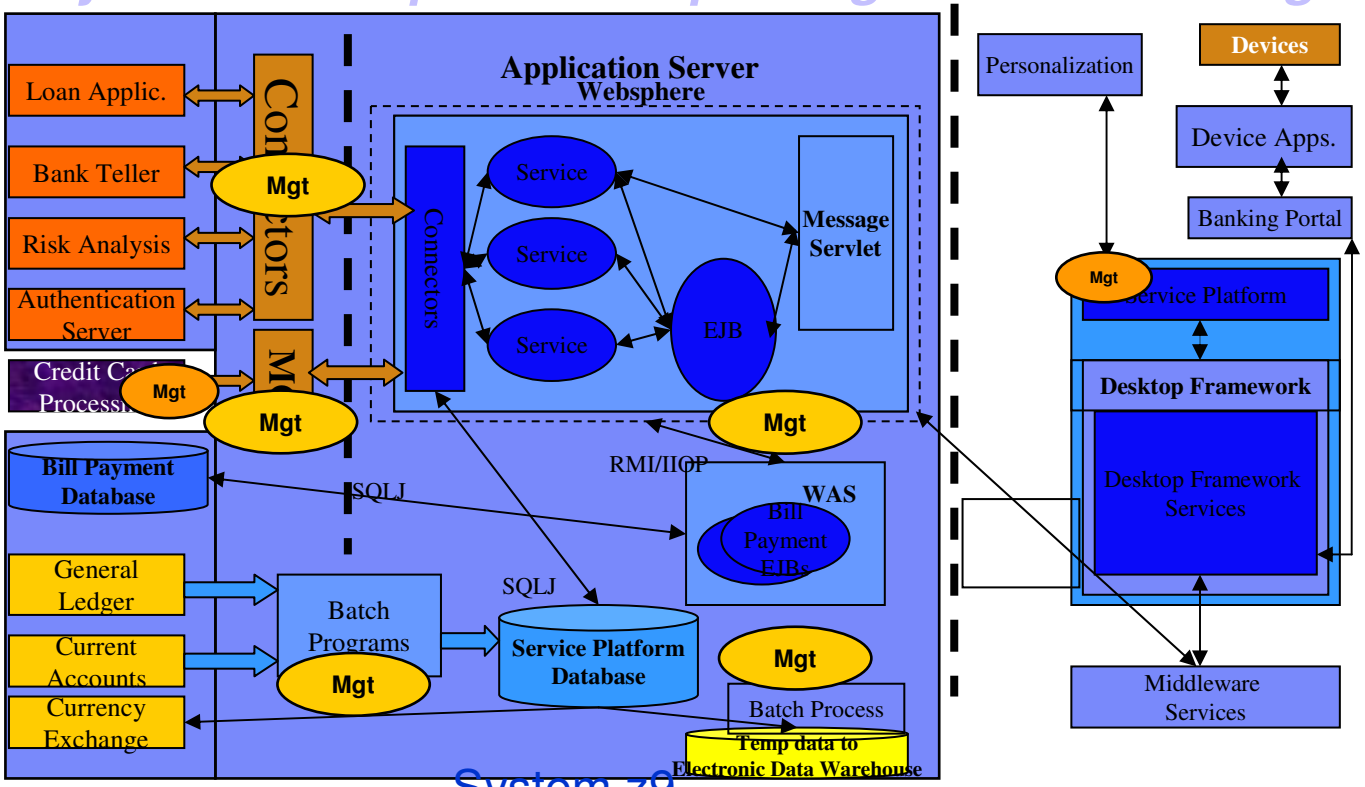
Typical multi-system Design: Numerous Mgmt Domains



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



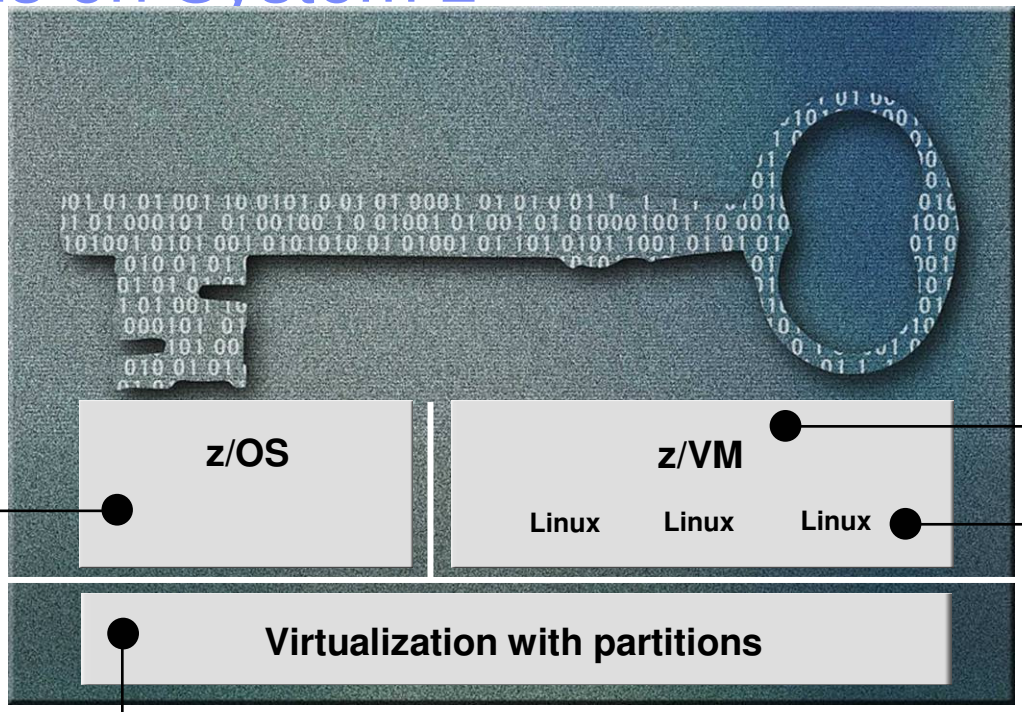
System z9

Potential advantages of consolidating your application and data serving

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

Certifications on System z

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



z/OS

- **Common Criteria** EAL4+ with CAPP and LSPP
  - z/OS 1.7 + RACF
- **IdenTrust™** certification for z/OS PKI Services

z/VM

- **Common Criteria** EAL3+ with CAPP and LSPP
  - **z/VM 5.1 + RACF**

Linux on System z

- **Common Criteria** EAL4+ with CAPP and LSPP
  - **SUSE LES9 certified**
- **Common Criteria** EAL3+ with CAPP and LSPP
  - **Red Hat EL3 certified at EAL3+**
  - **Red Hat EL4 EAL4+ in progress**

System z EC and other System z servers

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

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

z/OS System Testing

- We continually challenge our systems
  - **Using IBM's Hawthorne Research Lab Experts**
    - **Research keeps current with hacker sites, CERT, etc.**
  - **Test with and without the Firewall Technologies**
  - **Test at Component Test time**
  - **Test again under production load at Integration Test time**
  - **Fix potential exposures and test again**

Key System z Security opportunities

Category	Technology	Customer value	Customer ROI
Corporate Governance			
Audit, Reporting	Consul Insight	Consistency across Enterprise	Easier/faster reporting for SOX, HIPAA, Basel, etc
Data Protection			
Network Encryption	IPSec SSL/TLS	End to end encryption; Covers 'Last mile' Application level	zIIP exploitation reduces TCO; Transparent to applic.
Removable media	TS1120; Enc Facility	Tape, FTP risk mitigation	Encryption offload; Simplified distribution
Storage	Data Utilities, future disk	Data at rest	Avoid inadvertent disclosure
Authentication	PKI/Digital Certs	Crypto enabler; Industry standard	Low mips; avoids licensing costs; BR enabled
Consolidation via Virtualization			
Compartmentalization	PR/SM LPAR & zVM; z/OS MLS & processes	Reduced complexity; Tighter integration	Less environmentals, FTEs, improved MTBFailure, Capacity on Demand
Provisioning and Identity Management			
Registration of users	Consul zSecure; Tivoli Identity Mgr	Consistent processes for registration of users	Cloning; reduced human errors; faster deployment

In closing…

- **Mainframe superior economies and qualities of service include:**
  - Large scale performance for data intensive commercial environments
  - Unsurpassed virtualization capabilities
  - Built-in availability and resiliency for planned and unplanned outages
  - End to end security in the enterprise
  - State of the art automation
  - Excellence in centralized operation for simplified IT infrastructure
- **Ideal for Modernization, New Applications and Next Generation Systems:**
  - Modernize to drive business flexibility, enhance time to market and align business ant IT
  - Leverage existing application assets, corporate governance and skills
  - Transition to modern infrastructure capable of delivering Information on Demand built upon SOA
  - Replatform discussions with no change to underlying models and predicated on old client-server models are a relic of the past
  - Unleash the power of the mainframe to help you yield optimum TCO and maximum agility in the enterprise