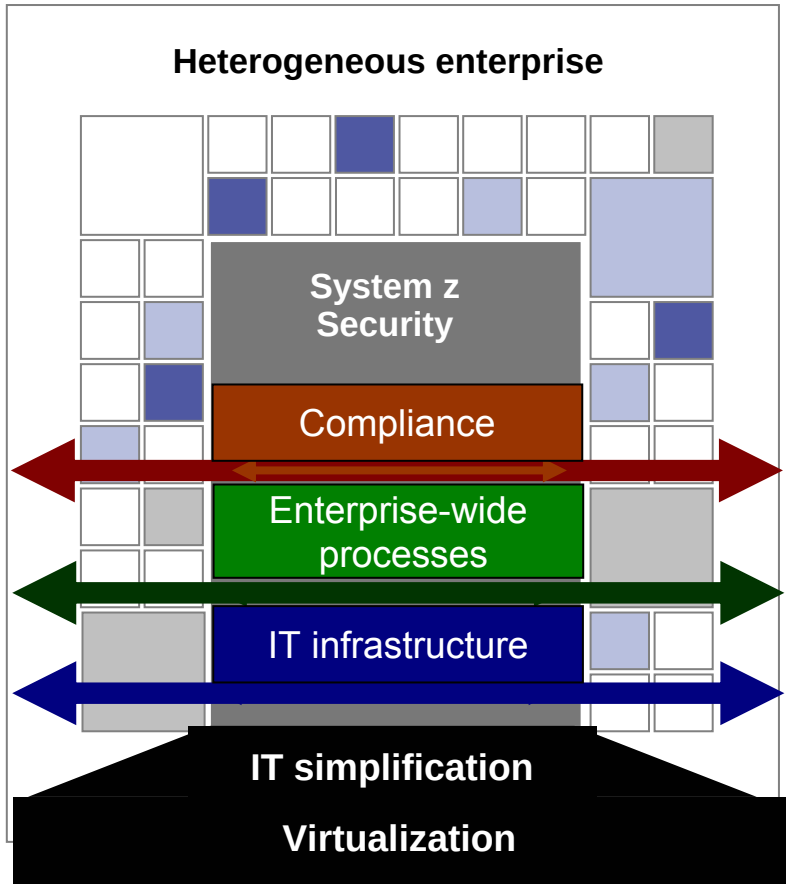
IBM Mainframe Security: An Overview

Jim Porell, IBM Distinguished Engineer

IBM mainframe security

Our goal is to continually **increase value** to protect our customers' investments by **extending** premiere System z **capabilities** across **heterogeneous platforms** to become the '**Enterprise Trust Authority**' for On Demand Business.



"Whilst the performance and resilience characteristics* (of the System z9 109) *are formidable, it is the security features that are likely to attract most attention"

Tony Lock – Chief Analyst, Bloor Research 2005

Why should I care?

What's at risk?

- Disclosure of sensitive data
- Service interruption
- Corruption of operational data
- Fraud and ID Theft
- Theft of services

What's at stake?

- Customer trust
- Reputation and Brand
- Privacy
- Integrity of Information
- Legal and Regulatory Action
- Competitive Advantage

Breach cost?

- $ Research and recovery
- $ notify customers
- $ Lost customer business
- $ Problem remediation
- $ Claims from trusted vendors and business partners

$$ Damage to brand image

What is Security from a customer view?

Security is not all about technology!
(it's really all about people)

- Policy
- Corporate Directive
- Regulatory Compliance (e.g. HIPAA, Sarbanes-Oxley)
- Technology (e.g. RACF, ACF2, Tivoli Access Manager)
- Infrastructure (e.g. Tivoli, Vanguard, Consul, Beta)
- Components (e.g. firewalls)
- Preventative (e.g. anti-virus, intrusion defense)
- Business workflow (e.g. Analytics, audit)
- Physical (e.g. Badge Access, Biometrics)
- Multi-media (e.g. Video cameras, voice analysis)
- Executive Position (e.g. CISO, CPO)
- Skill specialty (e.g. CISSP)
- Department (e.g. Info Assurance, IT Security)

- Typically, it's not → a Solution
  - Leverage Security to make solutions better
  - But there are new "offerings" evolving that look like solutions
    - e.g. DB2 Entity Analytics Solution

- Redundant
- Bureaucratic
- Too Sensitive
- Expensive
- Unresponsive
- Big Brother

Different People have different “security” needs

- Chief Information Officer
  - Are my systems and data protected from inadvertent disclosure?
  - Are best practices deployed for security?
  - Should I build or buy security?
- Chief Financial Officer
  - Total cost of ownership – how much does “security” cost?
  - What return on investment does this spending deliver?
  - What risks/costs does it avoid?
- Chief Privacy Officer/Chief Information Security Officer
  - Can I meet Regulatory Compliance needs?
  - Are our processes auditable?
  - Are my IT Operations, Developers, End users/consumers educated on our security practices?
- Application Architects
  - Do we design “security” into the application architecture, add it after the fact or leave it up to the IT Operations staff?
- IT Operations
  - What products and technologies will best meet the needs/requirements of all the “executives” that have a security/compliance/audit focus in the business?

The Facts – new era of computing is evolving

- Myth: 80% of mission critical data is on a mainframe
  - Reality – it's on x86/RISC too, because they made a copy.
    - We will never get to a single instance of data. However, z can be leveraged to reduce the number of instances of data and in doing so, assist to simplify governance and data protection.
- Customers require "integrity" based computing
  - System z's can now host the same code as other platforms (e.g. Java, J2EE, C/C++)
  - However, System z's architecture can greatly change the operations model
    - BR, Security, Storage Mgt, Business Process Integration, Workload and Capacity Mgt
    - Microsoft and Oracle talk. System z delivers with it's holistic design and deployment of Middleware, Operating Systems, Firmware, Hardware, Storage and Networks
- Operational Risk is now a Real Time requirement, not a post processing exercise.
  - System z makes you safer by enabling real time access to SHARED mission critical data, while meeting service levels and reducing the complexity of data moves, data protection and regulatory governance.
    - Where do those costs appear in a benchmark?
- Throw away your traditional spreadsheets for benchmarking Nextgen costs
  - System z specialty engines and operational characteristics change an application's Acquisition costs, upgrade costs and operations costs in ways that other server environments have yet to comprehend.

We need to break down the organizational barriers

- **IT Organization**
  - **OLTP**
  - **Database Serving**

- **"Distributed systems"**
  - **Web serving & Internet access**
  - **Business Intelligence**
  - **Storage Area Networks**
  - **Rapid Application Development**
  - **"just good enough"**
  - **Linux, Windows, UNIX**

We need to break down the organizational barriers

- **OLTP**
- **Database Serving**

- **Web serving & Internet access**
- **Business Intelligence**
- **Storage Area Networks**
- **Rapid Application Development**
- **"just good enough"**
- **Linux, Windows, UNIX, System z**

We need to break down the organizational barriers

OnDemand Organization

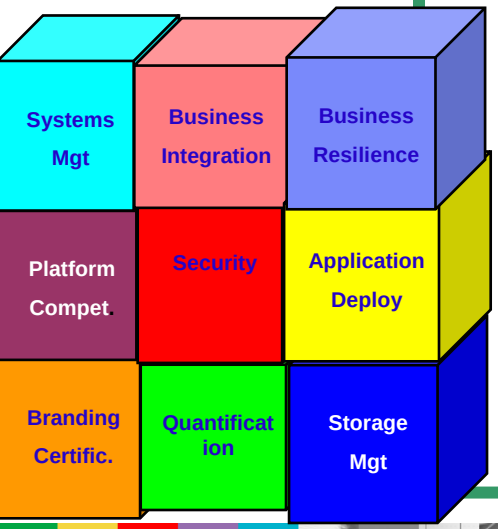
- •OLTP
- •Database Serving
- •Web serving & Internet access
- •Business Intelligence
- •Storage Area Networks
- •Rapid Application Development
- •"just good enough"
- •Linux, Windows, UNIX, System z

Phase 2

- Application Deployment
- Storage Vault
- Entity Analytics
- Hosted Clients

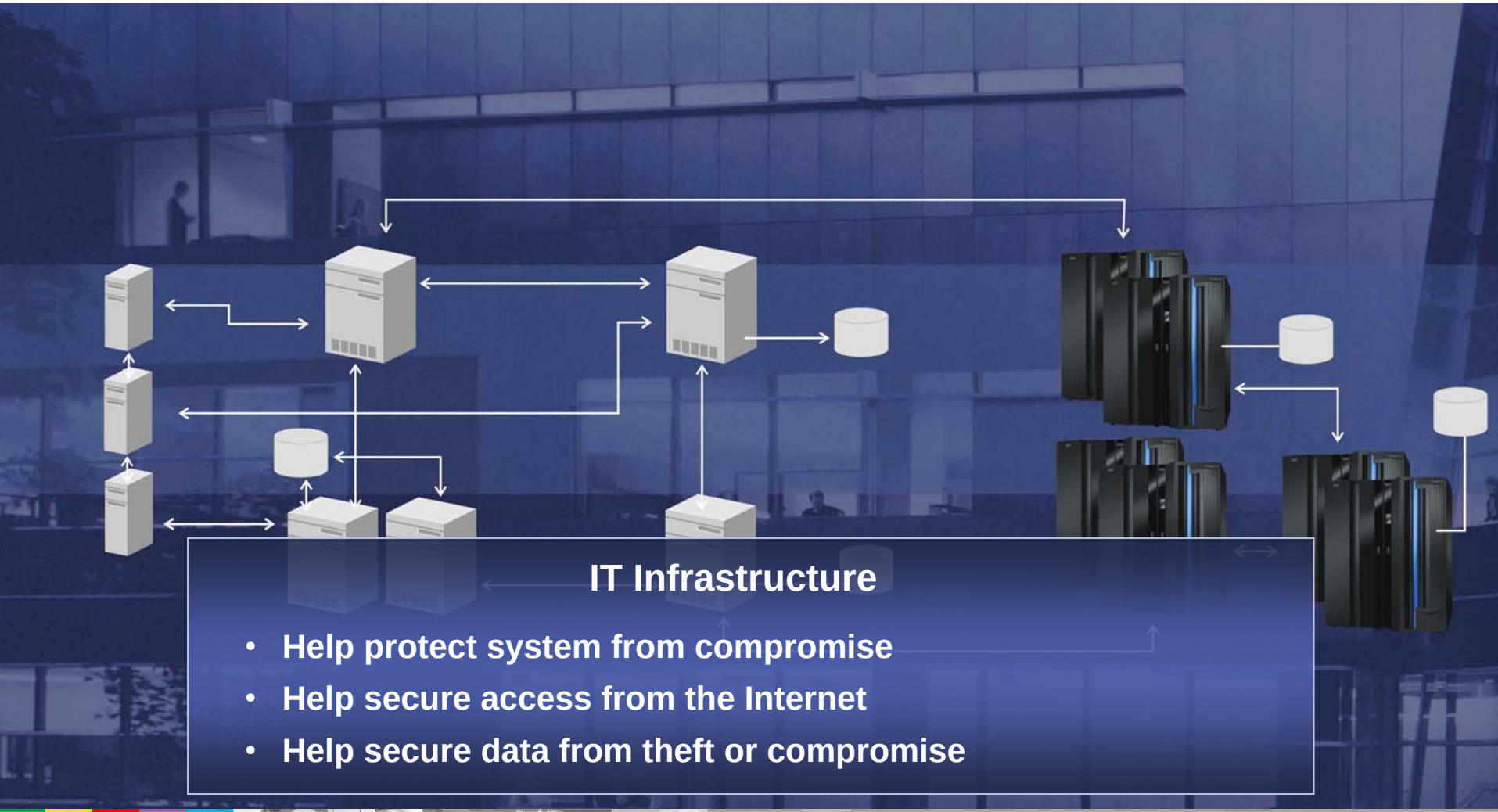
Phase 1

- Workload Integration
- Business Process Integration
- Security
- Business Resilience



Managing risk across the enterprise

The pillars of mainframe security

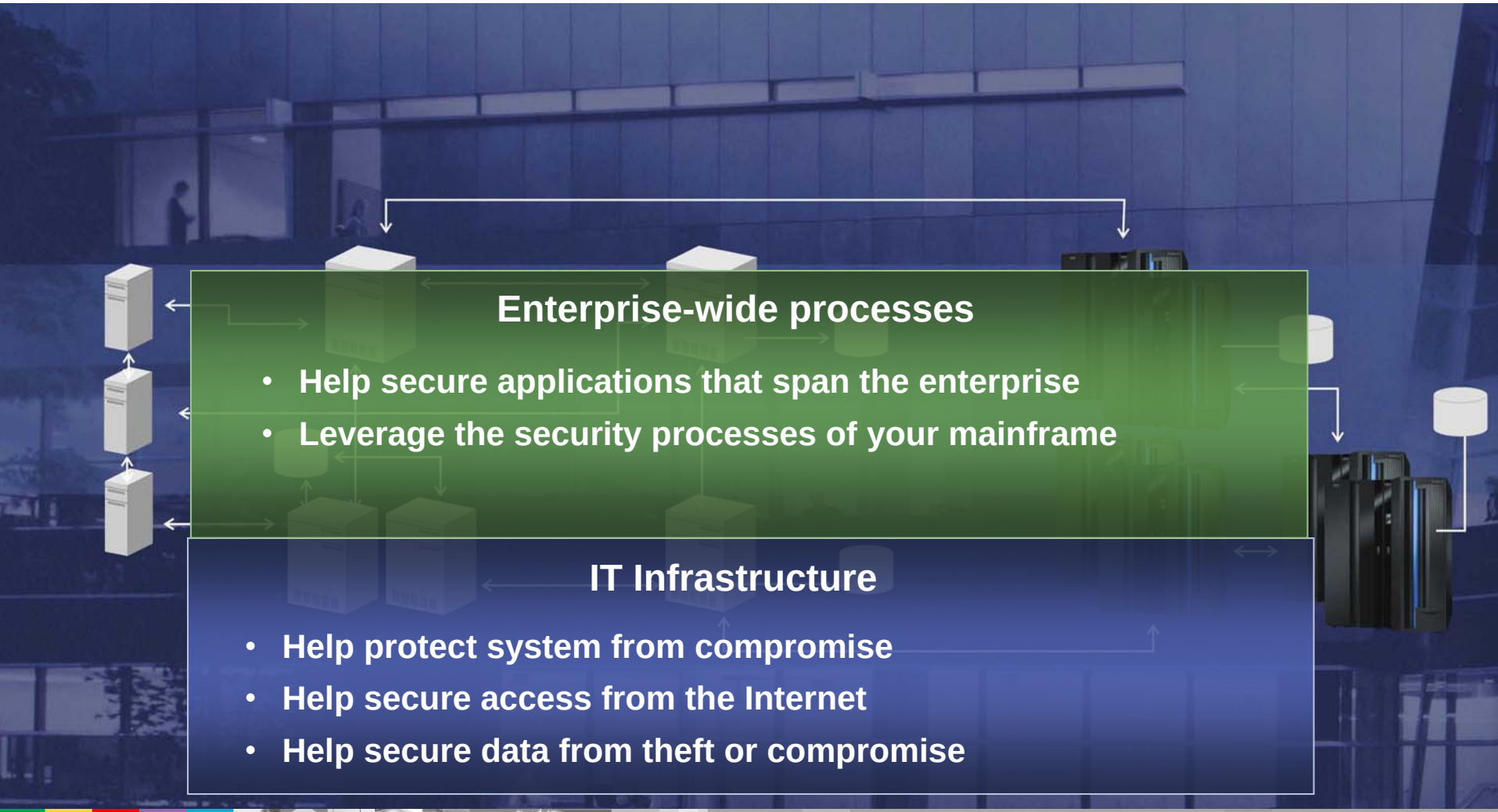


IT Infrastructure

- **Help protect system from compromise**
- **Help secure access from the Internet**
- **Help secure data from theft or compromise**

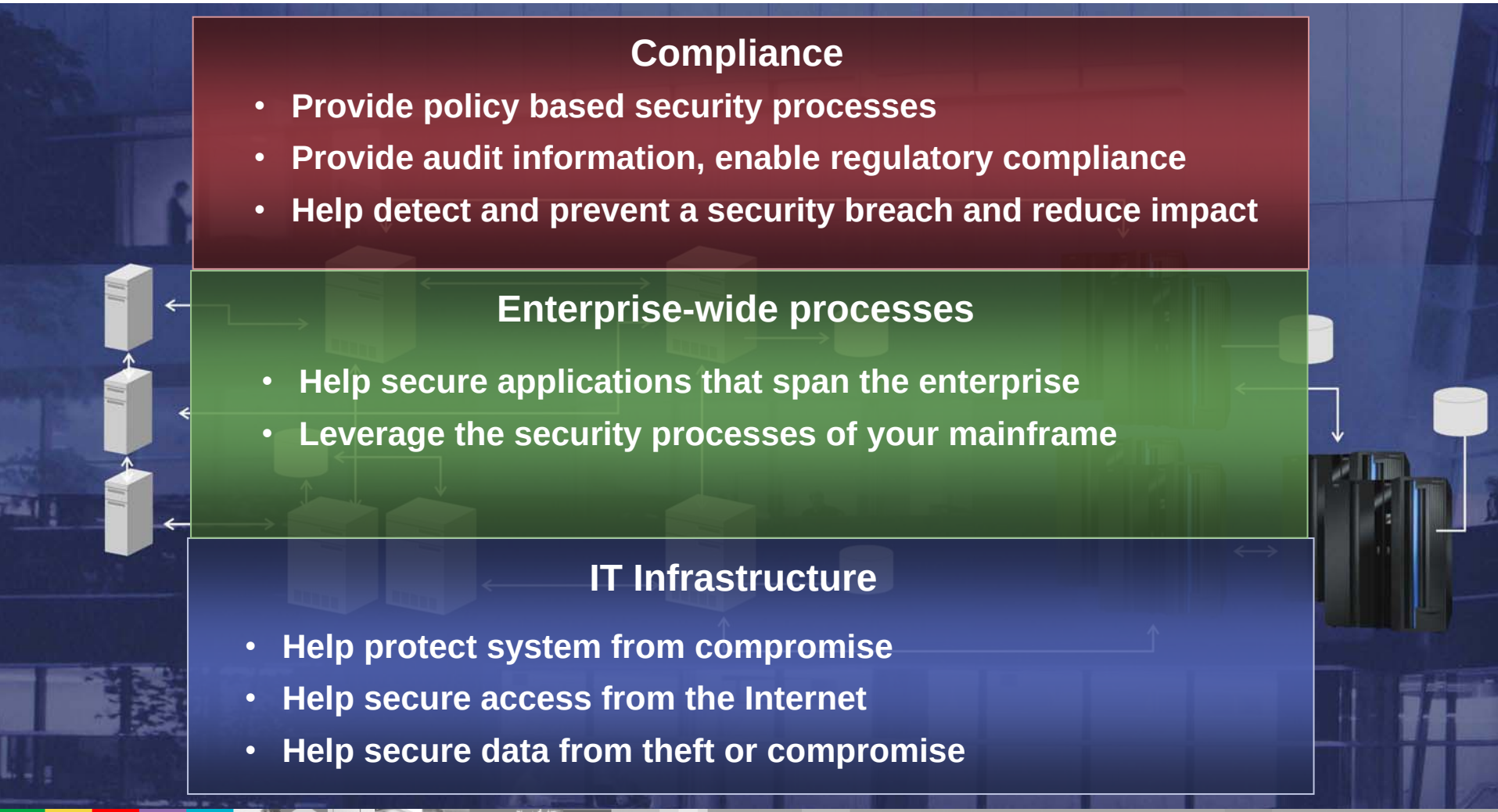
Managing risk across the enterprise

The pillars of mainframe security



Managing risk across the enterprise

The pillars of mainframe security



Protect sensitive information on line and off line

System z provides security without sacrificing responsiveness

- Protect the data
  - **End-to-end protection that helps keep data uncorrupted and uncompromised**
  - **Multiple Level Security for different levels of "need to know"**
- **Encrypt sensitive data**

- Prevent unauthorized access
  - **IBM Resource Access Control Facility – 25 years strong**
  - **Support for a variety of encryption algorithms**
  - **EAL5 and other security certifications**
- Secure and speed the transaction
  - **Specialized Cryptographic co-processor hardware**
- Monitor, manage, and control
  - **Centralized access and control helps lower security costs, meet compliance guidelines, and simplify audit trail.**
- Compliance with privacy/security legislation
  - **Auditability**
  - **Control**
  - **Recoverability**
- ISV solutions available
  - **Vanguard**
  - **Stonesoft**
  - **Consul Risk Management**
  - **More – from a large selection of ISVs**

Governance and Compliance

Governance, Compliance, Risk
(With a focus on policy)

- ***For organizations which need to***
  - Enable regulatory compliance
  - Ensure the accuracy of financial reporting
  - Preserve the integrity of data throughout its life cycle
  - Meet privacy requirements
  - Prevent fraud
  - Improve data governance.
  - Reduce risk of business process failure

Tooling

Z Products/features	Tivoli
z/OS itself	Access Manager
RACF	Identity Manager
SMF	License Manager
Health Checker	CARS component
Multi-level Security	Security Operations Manager
GDPS	
Vanguard	
Consul	

Service Offerings:

Diagnostic Health Checks can front end any service

Service to build a Compliance platform for: reporting, auditing, preventative controls, risk reporting, risk modeling, core banking

Data Governance Services, data management, data transformation

Privacy related services to deploy Sparcle

Secured Process

Security Process Management
(Progressively Autonomic)

- ***For organizations which need to:***
  - *Secure solutions that span the enterprise.*
    - leveraging the proven security processes of your mainframe
  - *Extend their mainframe security investments to new SOA applications.*
  - Secure applications throughout their development cycle
  - *Reduce complexity, reducing vulnerabilities, automating security processes*
  - *Evolve from a reactive approach to a predictive security approach.*
  - *Access secured and encrypted data repositories*
  - *detect and prevent a security breach and reduce impact*
- ***In sum, organizations must stop the bleeding, take protective measures and reach a self healing security state.***

Tooling

Z Products.features	Tivoli
Workload Manager	Access Manager
LPAR	Identity Manager
Common Criteria	Federated Identity Manager
PKI - Digital Certificates	CARS Component
Enterprise Identity Mapping	Compliance Management
Communications server - IDS	DataPower
Vanguard Consul	

Service Offerings:

SOA security services - build SOA architecture

PKI services planning and deployment

Encryption services

Establishing Websphere security services

Secured Infrastructure

Secure Infrastructure
(Network, Information, Application)

- ***For Organizations which need to:***
  - *Protect System from Compromise*
    - Have a resilient virus free infrastructure
  - *Have a consistent security fabric from distributed to mainframe*
  - *Have consistent auditing and reporting*
  - *Defend the network- Both intrusion detection and intrusion defense*
  - *Authentication and identity/provisioning to accommodate a spectrum of platforms, users, resources.*
  - *Secure eBusiness applications with digital certificates.*
  - *Secure Data from theft or compromise*
    - Ensure encrypted data transmission to clients and partners
  - *Have processing integrity across business transactions*
  - *Prevent fraud and malicious attacks*

Tooling

Z Products/features	Tivoli
RACF-LDAP	Access Manager
Passtickets	Identity Manager
Enterprise Identity Mapping	Federated Identity Manager
Encryption	Directory Integrator
PKI-Digital Certificates	Access Manager for enteprise Single Sign On
Communication server-IDS	
Application Transparent SSL/TLS	
Kerberos support	
Vanguard	
Consul	

Service Offerings:

Security architecture and deployment planning

Migration services from ACF2/TS/Other to RACF

Integration services between Tivoli and RACF

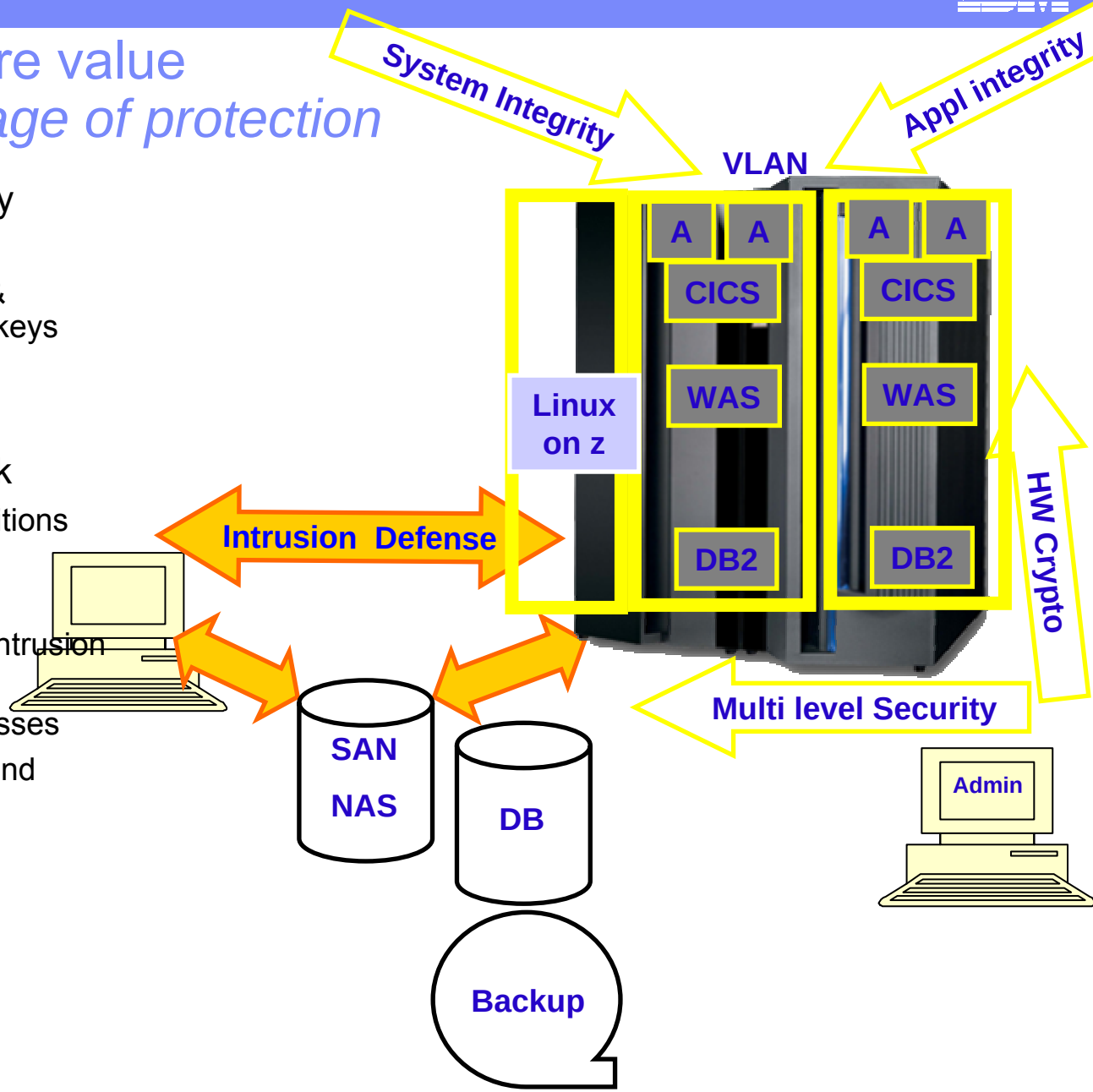
PKI services

Business continuity/GDPS

Fraud detection and forensic services using both Entity Analytics and other tooling

System z 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



The Power of Encryption

Helping to reduce risk across your value-net

Helping to protect data over the Internet

Helping to protect data leaving your enterprise*

Enterprise-wide Key Management

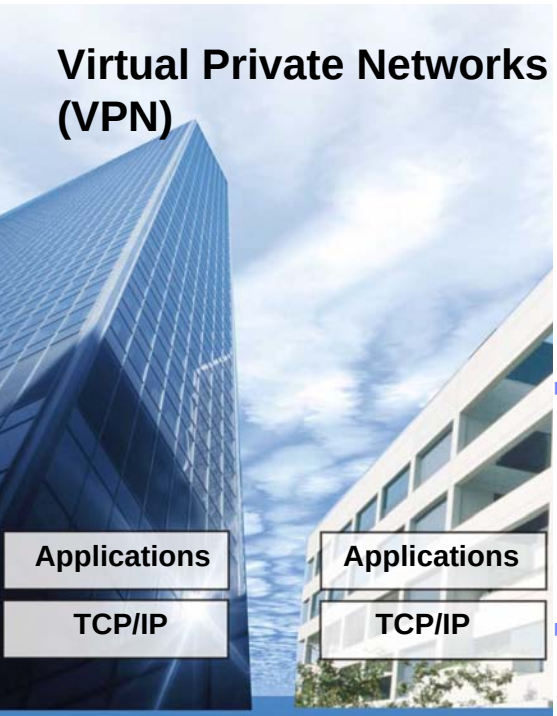
Helping to protect archived data*

Customer objectives:

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

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

Network security – z/OS intrusion detection services

Help secure access from the Internet

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**
- **New in z/OS 1.8:**
  - **No longer requires LDAP**
  - **Configuration assistant**

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

Tape encryption with System z in the enterprise

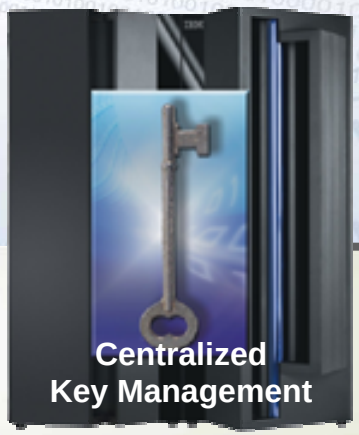
Help secure data from theft or compromise

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

Encryption Facility for z/OS, V1.1

Data Encryption in the Server



- Flexible options for business partner exchange
- Partners can encrypt and decrypt using no-charge JAVA client
- Supports public key or password based exchange

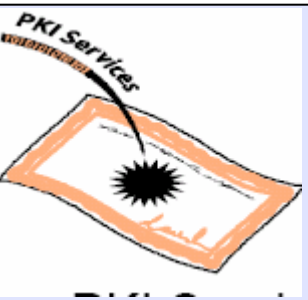
Data Encryption in TS1120

Enterprise scope

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

Digital certificate hosting on System z

Provide an identity authentication process



A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web.

A certificate authority (CA) is an authority in a network that issues and manages digital certificates.

CA often provided by third parties.

z/OS PKI Services to enable a Certificate Authority solution

- **Ability to host Digital Certificate management for the banks, government agencies…**
- **TCO advantage - no need to pay a third party CA for certificates**
- **Relatively low mips to drive thousands of certificates**
- **Scalable (Sysplex exploitation)**
- **Secure with System z cryptography (Secure Key)**

Used by large finance institution to save an estimated $16M a year

Provide access to data based on need to know

Multilevel Security

REQUIREMENT:

Data shared between people/organizations with different "need to know"

System z solution:

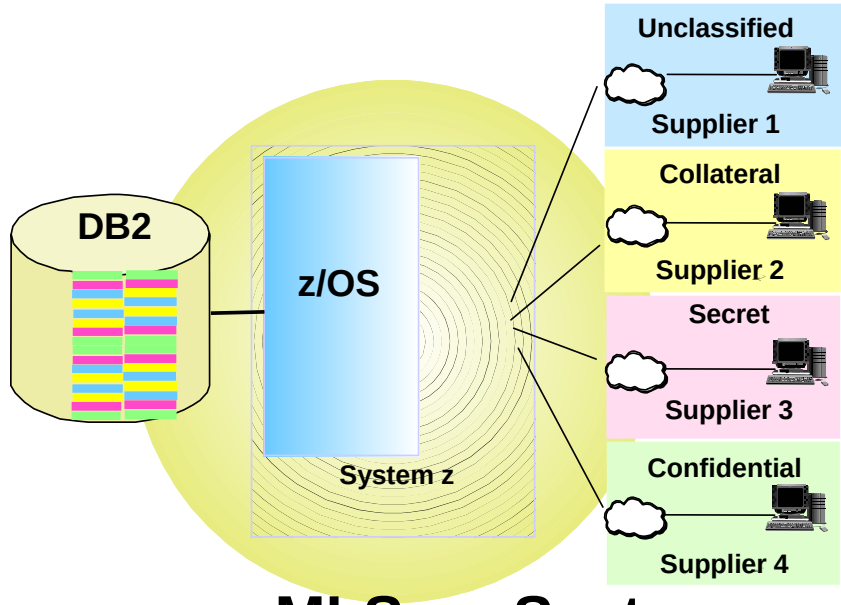
- Highly secure access to a single DB2 database
- Security labeling at the row-level of DB2
- With RACF as single security manager for both z/OS and DB2

Public Sector: Hierarchical security

- Commercial opportunities:
  - Hosting similar applications
  - Single database

    hosting subsidiaries

    hosting partners

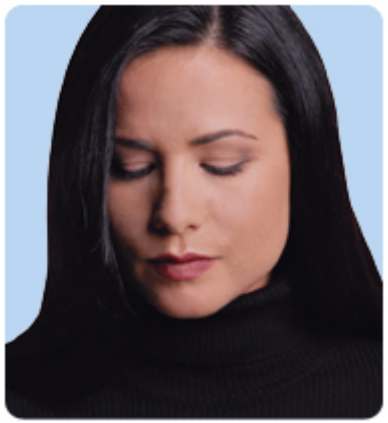


MLS on System z

Imagine the possibilities!

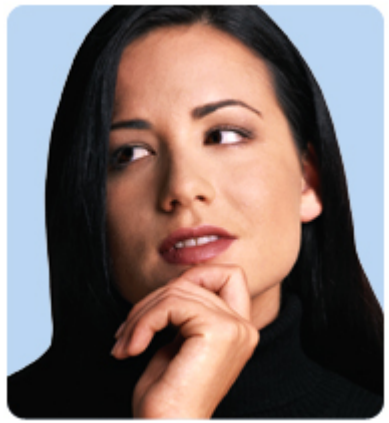
DB2 Identity Resolution Determines "Who is Who?"
Leveraging System z for Operational Risk

DB2 Identity Resolution software helps organizations recognize the single identity who is using multiple identities. So not just "Matching" but beyond "Matching" to finding individuals who are hiding and fraudulent.



Mrs. Kate Greene
1 Bourne St
Clinton MA 01510
Tel#978-365-5312
EIN#097376156
DOB 07/08/64
PPN# 068588345
LIC#1702188364

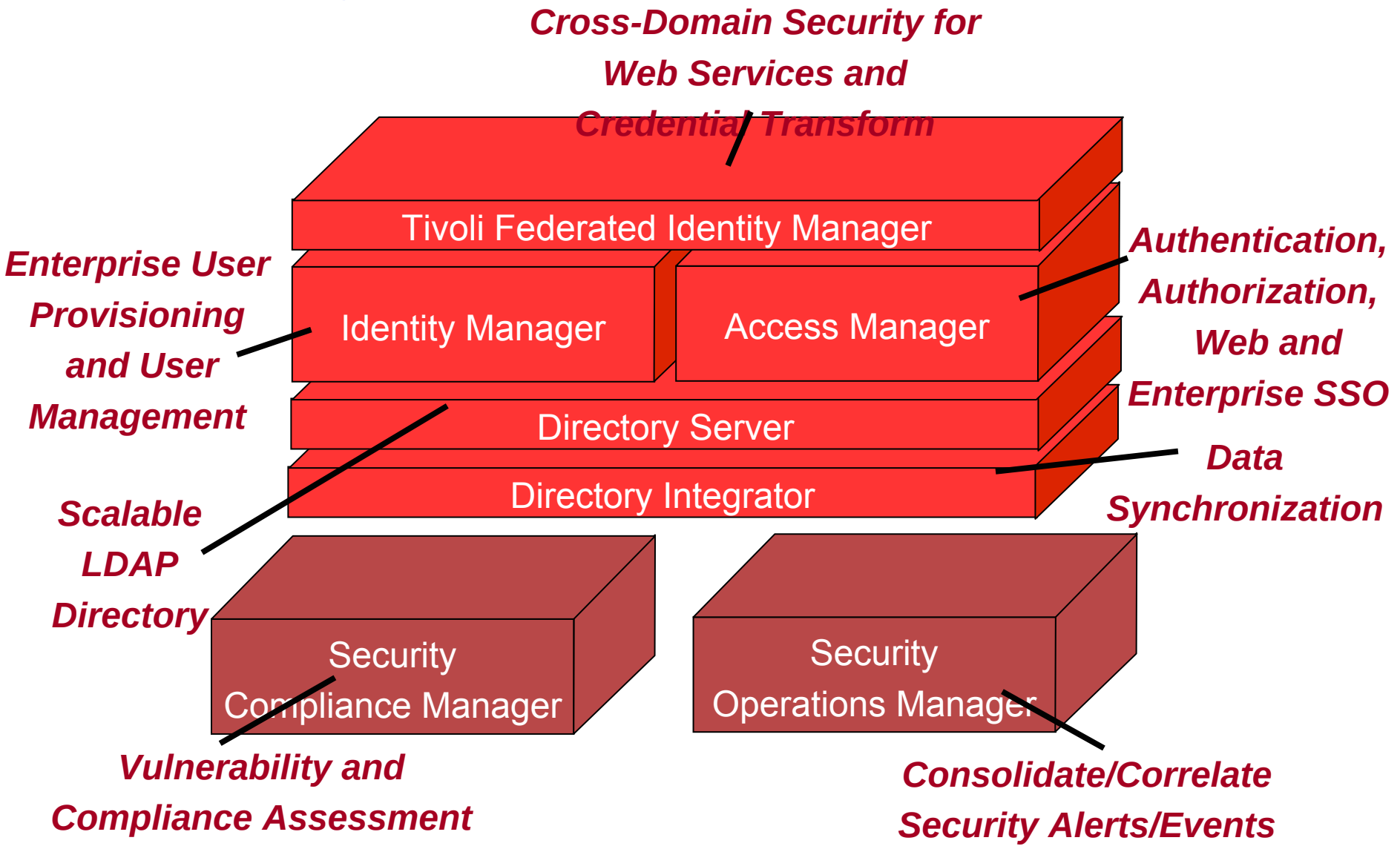
Mrs. Kathy Green
10 Bouren St
Clifton MA 01510
Tel#978-365-5312
LIC#1702188364
PPN# 0**86**588345



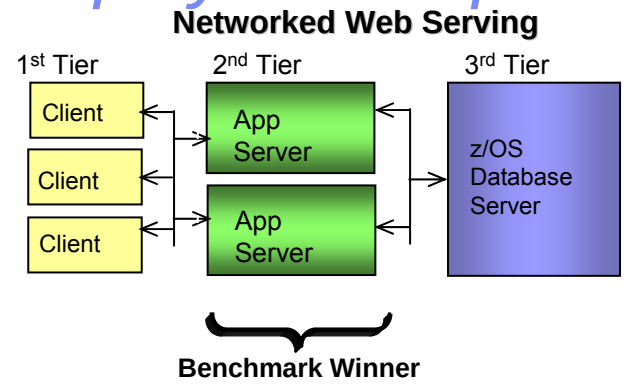
Ms. Katherine Green
1 Bourne St
Clinton MA 01510
TEL#978-365-**6631**
LIC#1702188364
DOB 07/**09/66**
EIN#097376156

Mrs. Kate Jones
APT 4909
Bethesda, MD 20814
Tel#301-654-5404
LIC#1702188364
DOB 07/08/64

Tivoli Security Product Portfolio



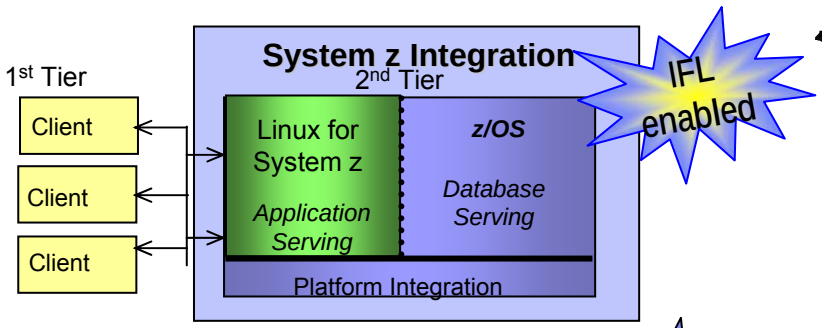
Simplify and improve TCO by integration



Route 9

Parkway

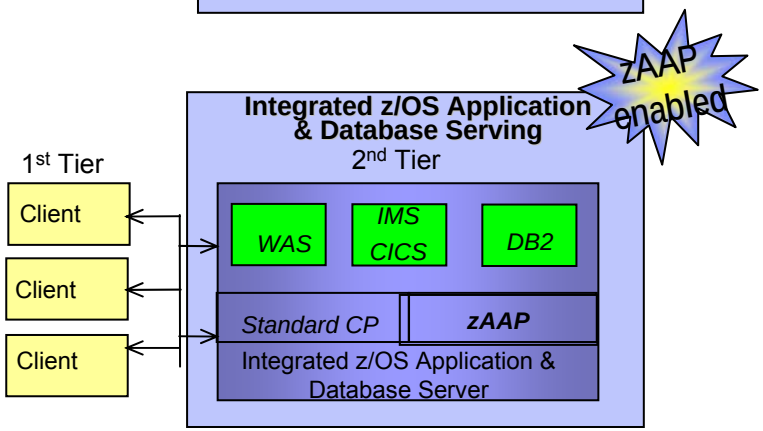
Advantages of consolidating your application and data serving



Better Production Value

- ✓Security — Fewer points of intrusion
- ✓Resilience — Fewer Points of Failure
- ✓Performance — Avoid Network Latency
- ✓Operations — Fewer parts to manage
- ✓Environmentals — Less Hardware

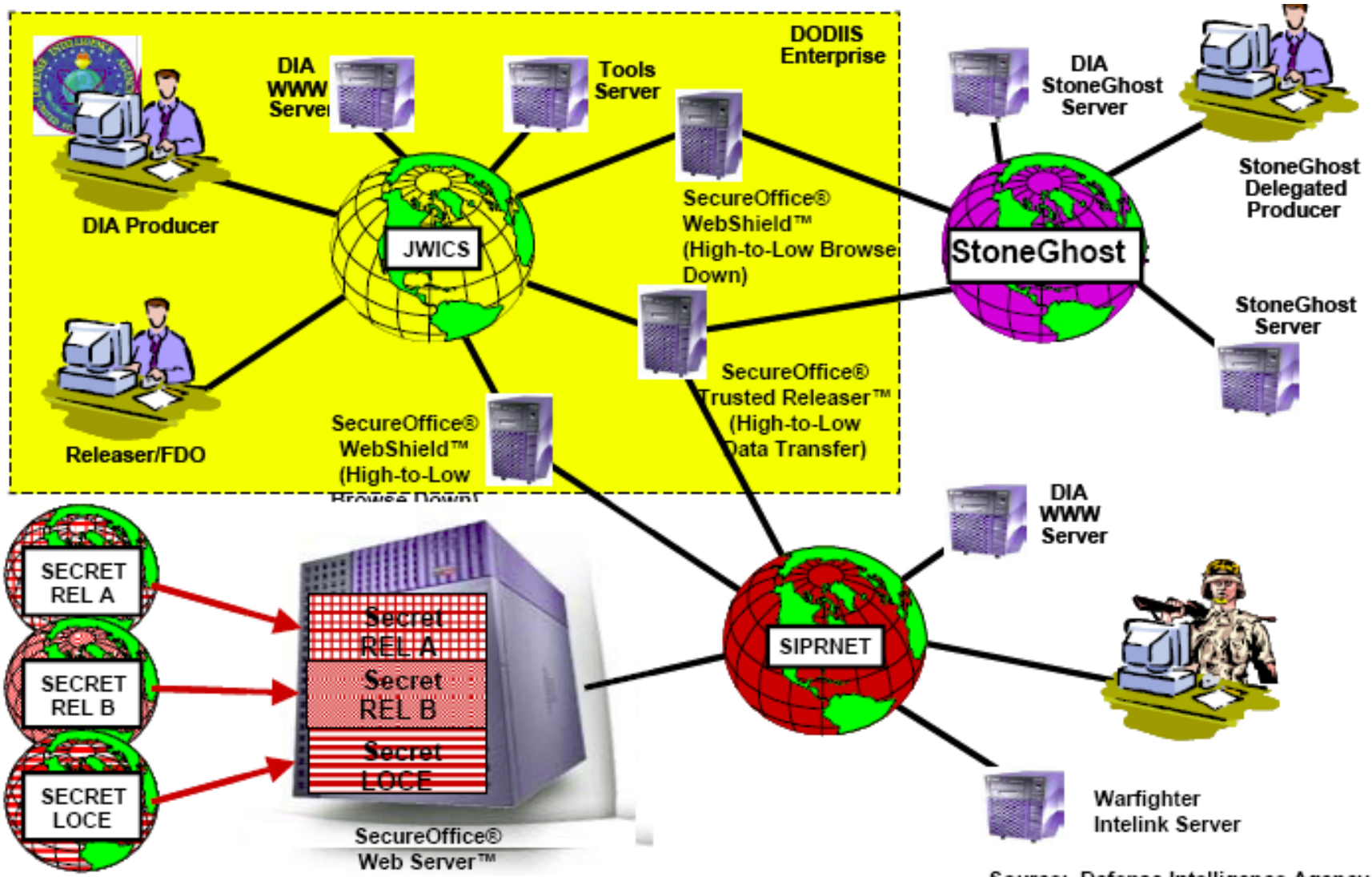
Interstate Highway



Best Production Value

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

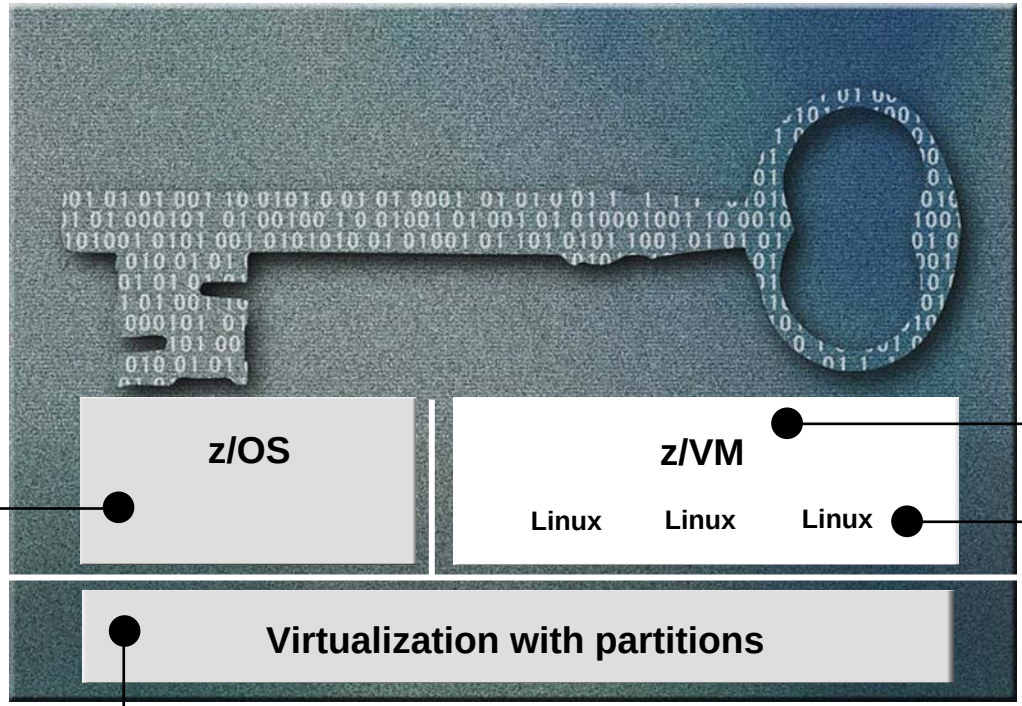
Stand alone servers



Source: Defense Intelligence Agency

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

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

z/VM

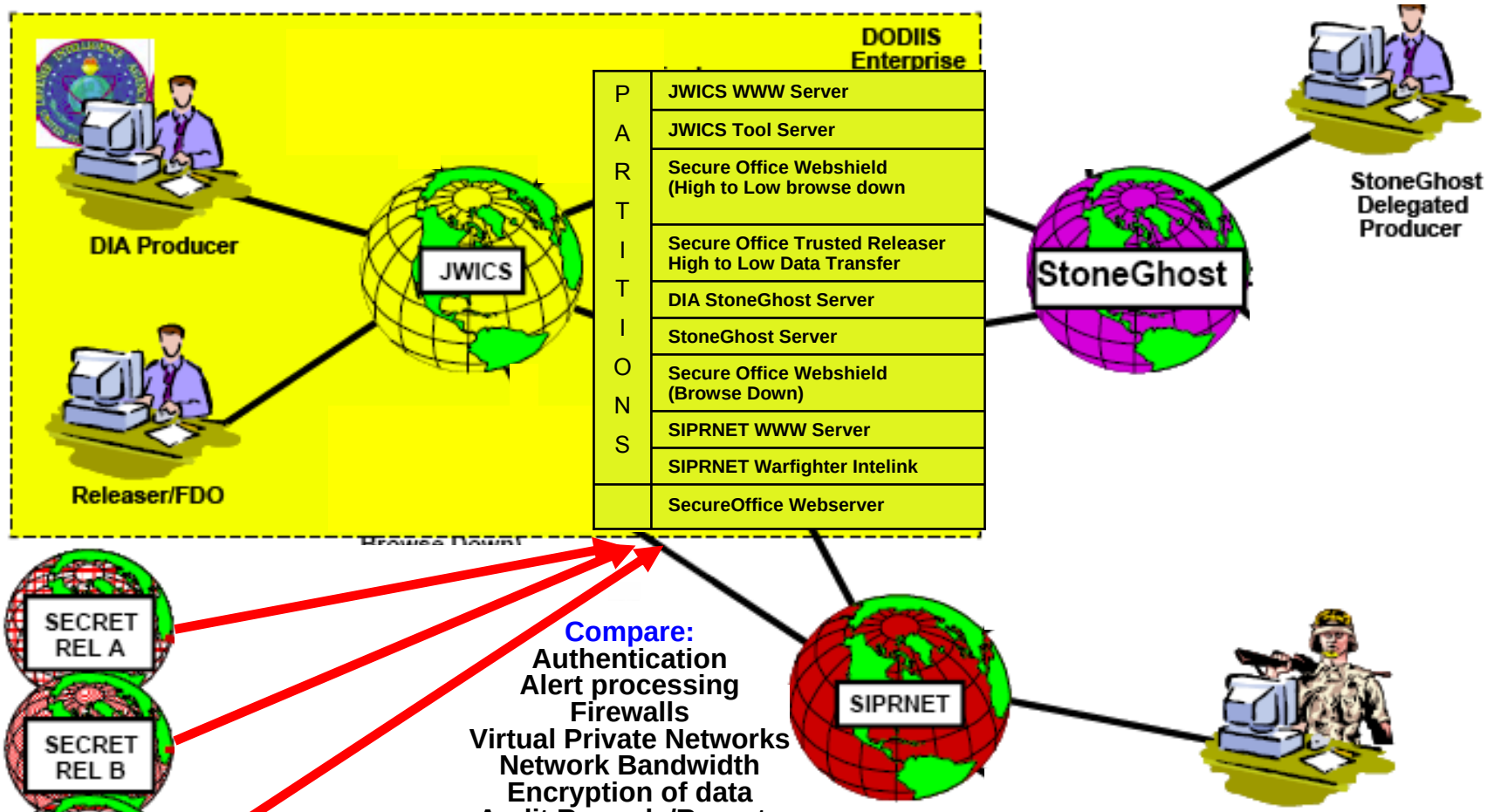
- **Common Criteria** EAL3+ with CAPP and LSPP
  - **z/VM 5.1 + RACF**

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**

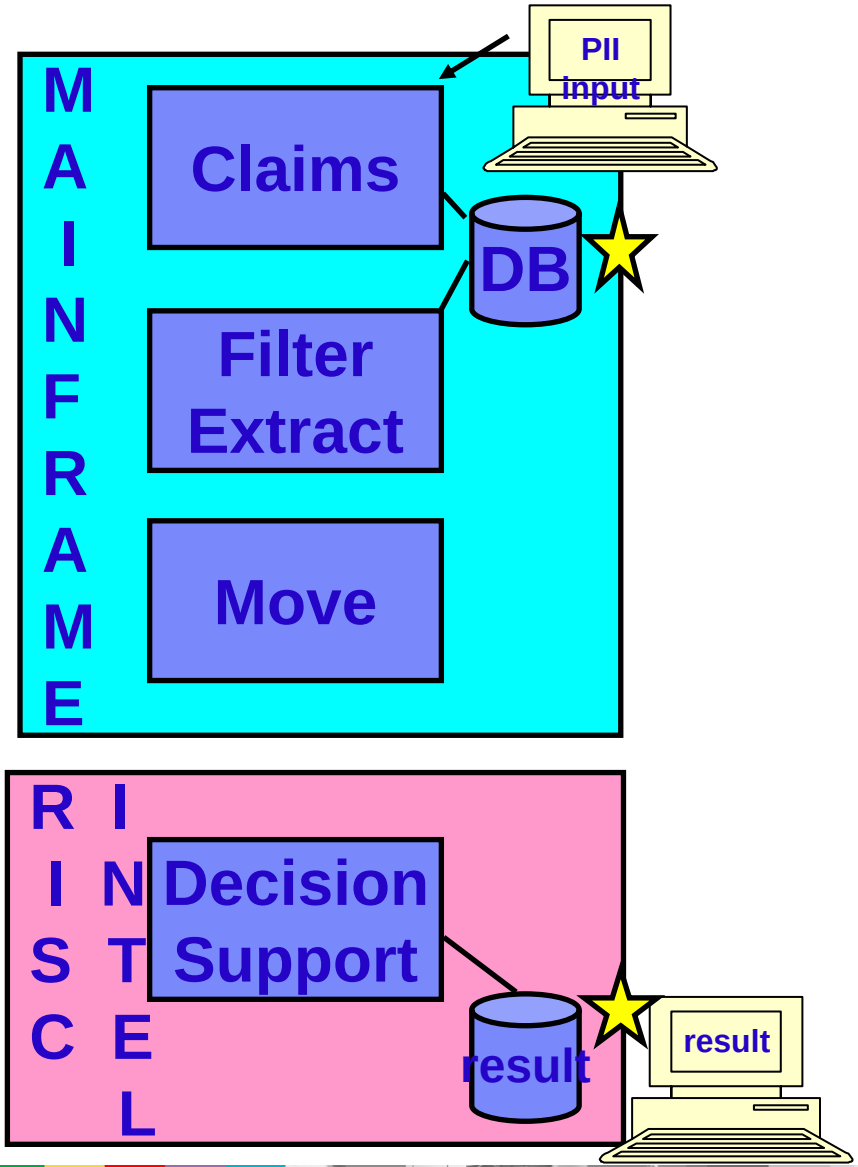
See: www.**ibm.com**/security/standards/st_evaluations.shtml

Consolidated Servers



This changes the economics and operational model

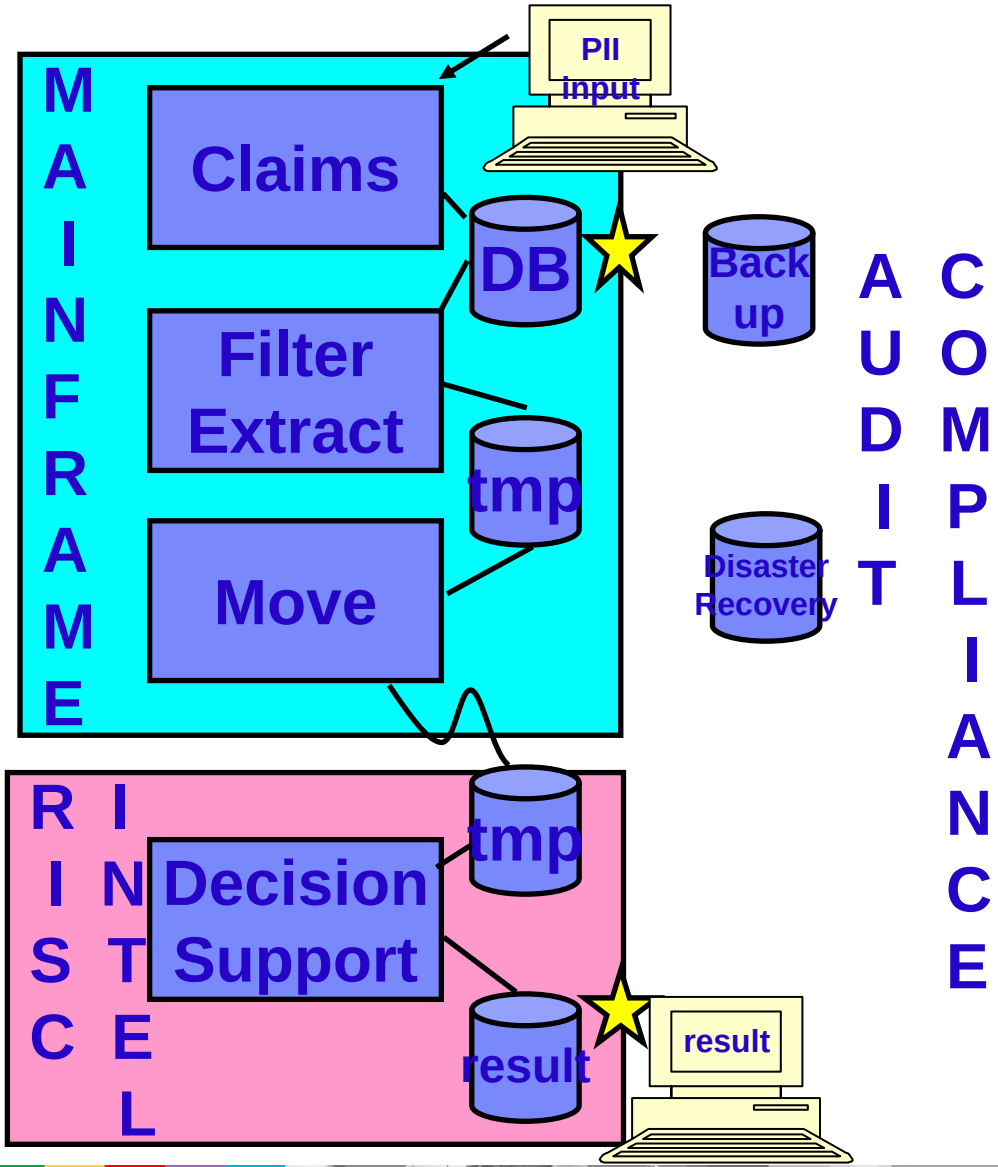
Why does Infrastructure simplification matter? HIPAA, Sarbanes-Oxley



Typical Business Workflow

- Do you audit all places with Personally Identifiable Information?
  - Is the process automated?

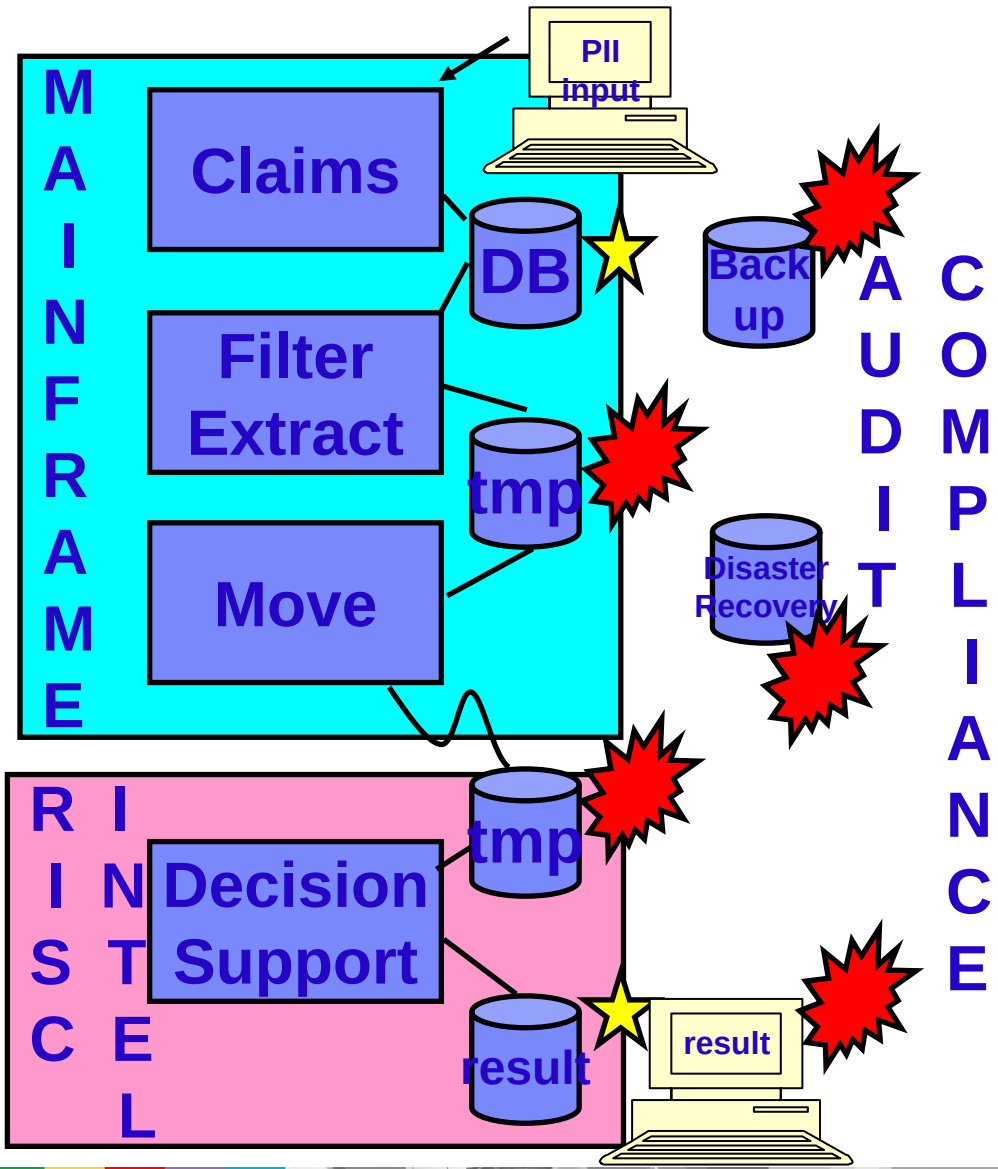
Why does Infrastructure simplification matter? HIPAA, Sarbanes-Oxley



Typical Business Workflow

- Do you audit all places with Personally Identifiable Information?
  - Is the process automated?
- Data is easy to replicate

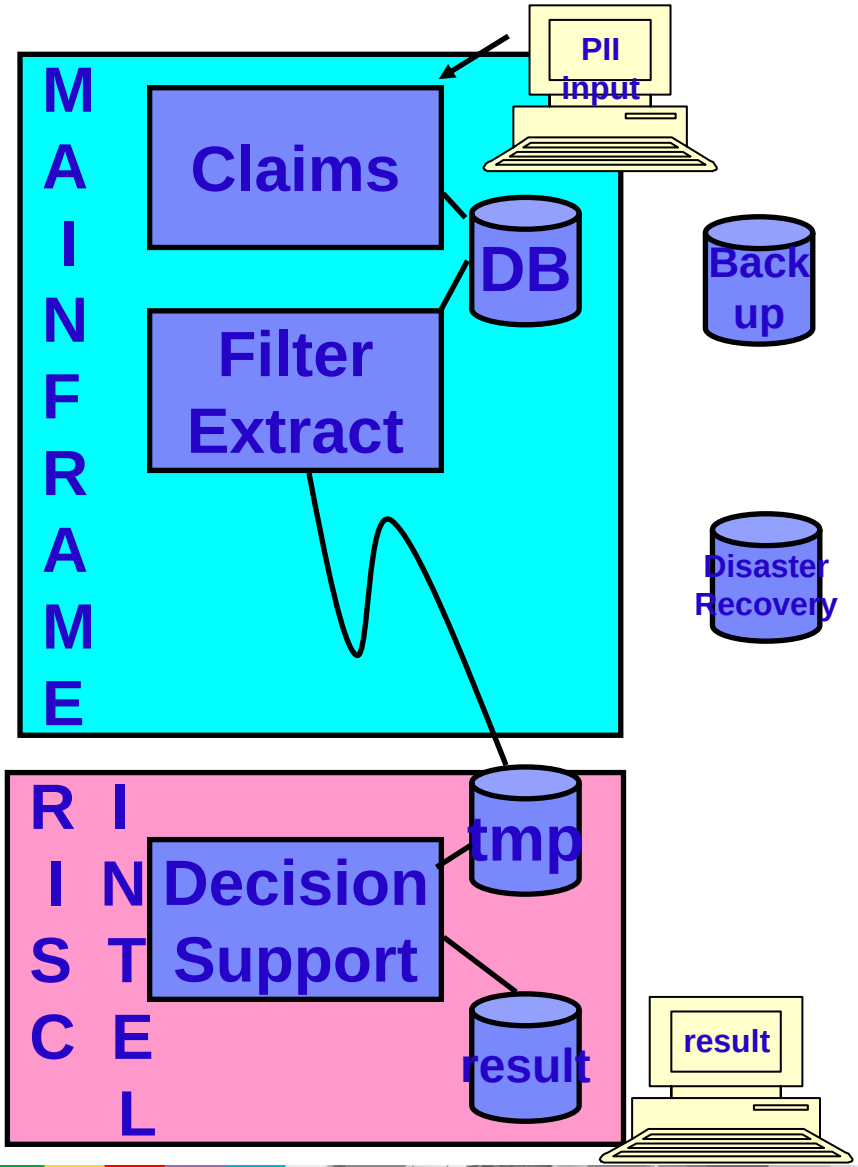
Why does Infrastructure simplification matter? HIPAA, Sarbanes-Oxley



Typical Business Workflow

- Do you audit all places with Personally Identifiable Information?
  - Is the process automated?
- Data is easy to replicate
- Policies are not.
  - Reducing the copies will reduce compliance efforts and increase resiliency

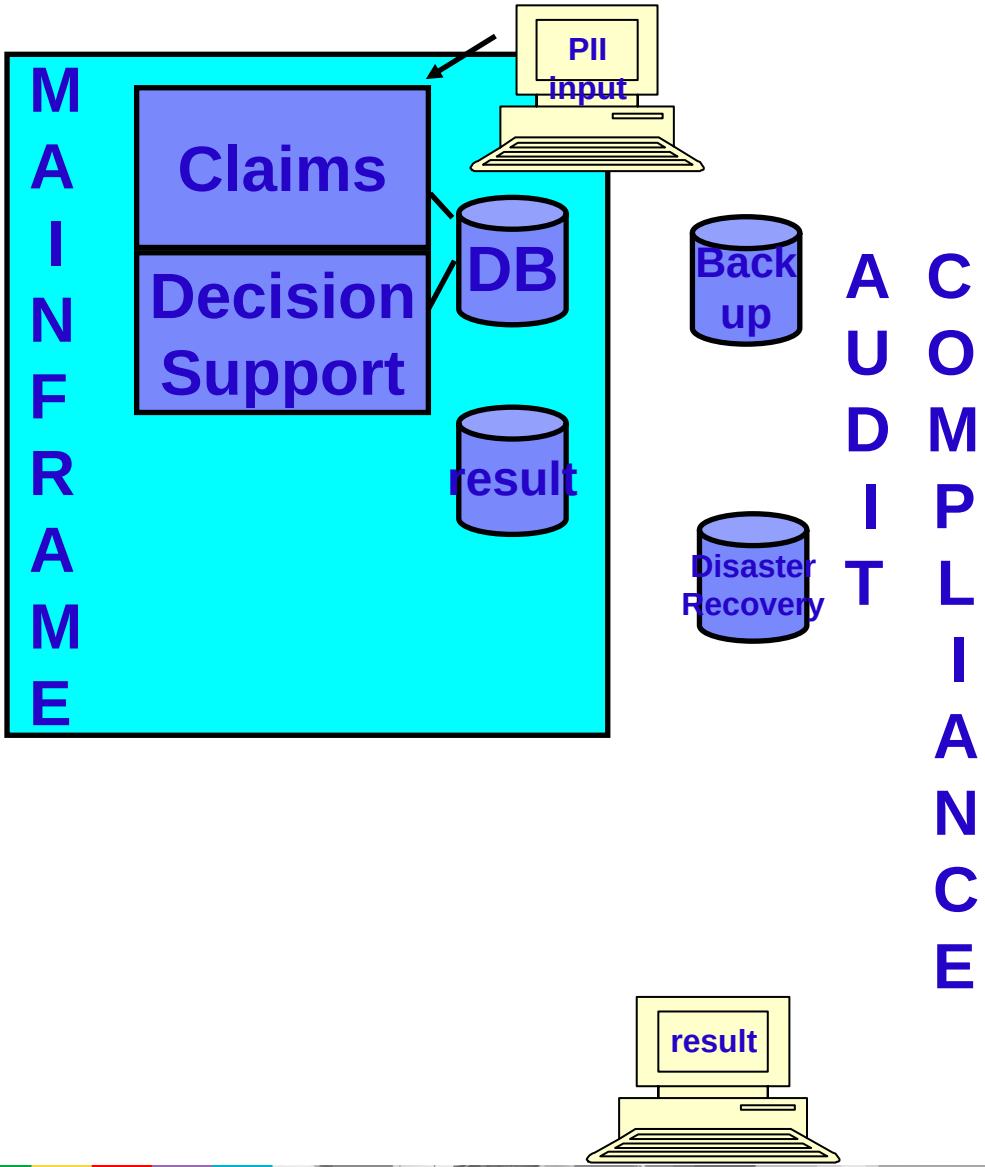
Why does Infrastructure simplification matter? HIPAA, Sarbanes-Oxley



Typical Business Workflow

- Do you audit all places with Personally Identifiable Information?
  - Is the process automated?
- Data is easy to replicate
- Policies are not.
  - Reducing the copies will reduce compliance efforts and increase resiliency
    - Leverage a file server to delete copies and reduce data movement

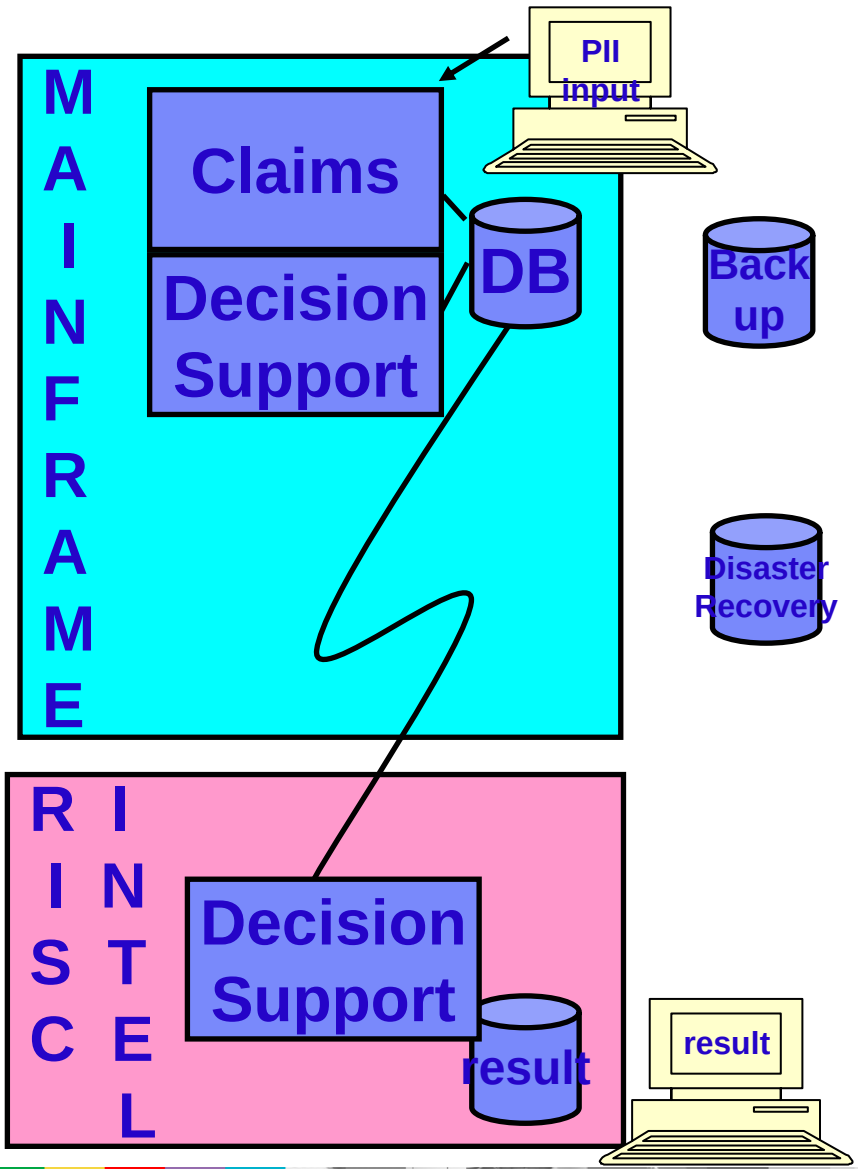
Why does Infrastructure simplification matter? HIPAA, Sarbanes-Oxley



Typical Business Workflow

- Do you audit all places with Personally Identifiable Information?
  - Is the process automated?
- Data is easy to replicate
- Policies are not.
  - Reducing the copies will reduce compliance efforts and increase resiliency
    - Leverage a file server to delete copies and reduce data movement
    - Application data proximity

Why does Infrastructure simplification matter? HIPAA, Sarbanes-Oxley



Typical Business Workflow

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

System z: The Data Vault

Enterprise Opportunities with z/OS and System z

- **Business resilience** - leverage System z to help fail over (DR) other servers' data
- **The vault** - how data can be referenced from System z (like DB2) for other servers, but with Integrity, Security and Resilience – simplifying Policy – HIPAA, Sarbanes-Oxley
- **Trust Authority for the enterprise** - identification and authentication, audit/compliance, Root Certificate Authority (saving real $) – Consolidating Audit records
- **Ethical Hacking** – ensuring security of operational deployment
- Leverage current assets – build Web services on the mainframe
- Utilizing the **zAAP, zIIP – changing the economics** for deploying on the mainframe
- **Infrastructure Simplification** – SNA consolidation, sharing applications
- SMB - the scale and manageability of the mainframe, but delivered in containers suitable for the SMB (on demand!)
- **Virtual Blade Center** - Fidelity's experience with provisioning Linux and their TCO vs. Intel boxes
- A z on every **developers desktop** - make the platform accessible to every developer via zVM or zEmulation on a PC.
- **Unlimited growth** - the answer is 64 bit.....move those old boxes up to z990's to prepare for z/OS 1.6
- ***The mainframe is a weapon, use it wisely***
  - **Cultivating growth opportunities**

IBM System z9 Security
Protecting an Enterprise

Helping to protect data over the Internet

Governance and Compliance

Vanguard, Tivoli Compliance
Identrus, Common Criteria, FIPS

Security Process Management

Vanguard, Tivoli Identity Manager
Intrusion defense services

Helping to protect data leaving your enterprise

Centralized Key Management

Helping to protect archived data

Customer objectives:

- Information Integrity
- Simplifying regulatory compliance efforts
- Secure exchange of business critical and sensitive data

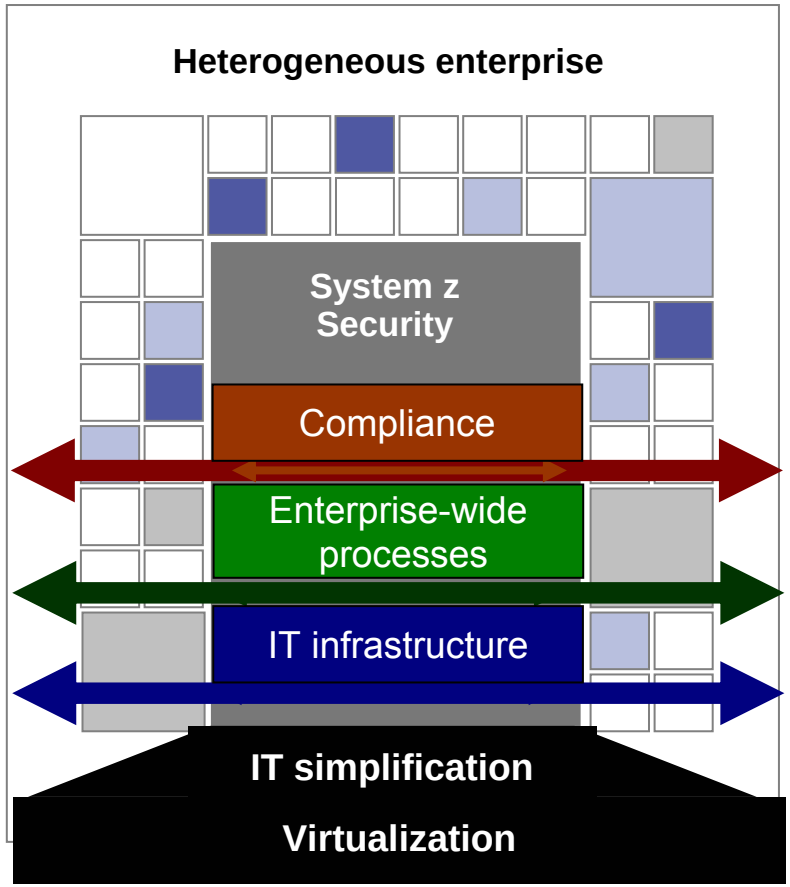
Secure Infrastructure

Data, Transaction & Network protection
PKI, LDAP, RACF, ssh, Cryptography

Helping to protect

IBM mainframe security strategy

Our goal is to continually **increase value** to protect our customers' investments by **extending** premiere System z **capabilities** across **heterogeneous platforms** to become the '**Enterprise Trust Authority**' for On Demand Business.



"Whilst the performance and resilience characteristics* (of the System z9 109) *are formidable, it is the security features that are likely to attract most attention"

Tony Lock – Chief Analyst, Bloor Research 2005

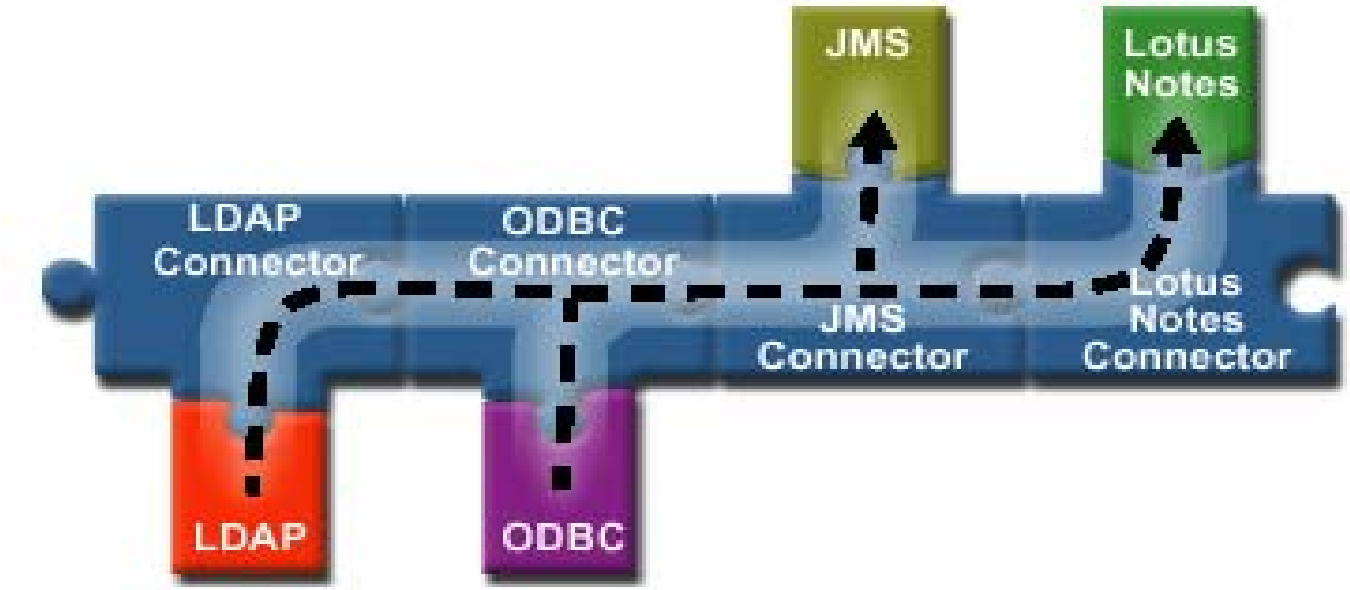
jporell@us.ibm.com

The Mainframe –
A History of Encryption Innovation

- Hardware Cryptography: 1970
- RACF: controls access to resources and applications – 1976
- Key management built into operating system (ICSF) – 1991
- PKI: create digital certificates & act as Certificate Authority – 2002
- Application transparent TLS – z/OS 2005
- Encryption Facility for z/OS: 2005
- Encrypting Tape Drive TS1120: 2006

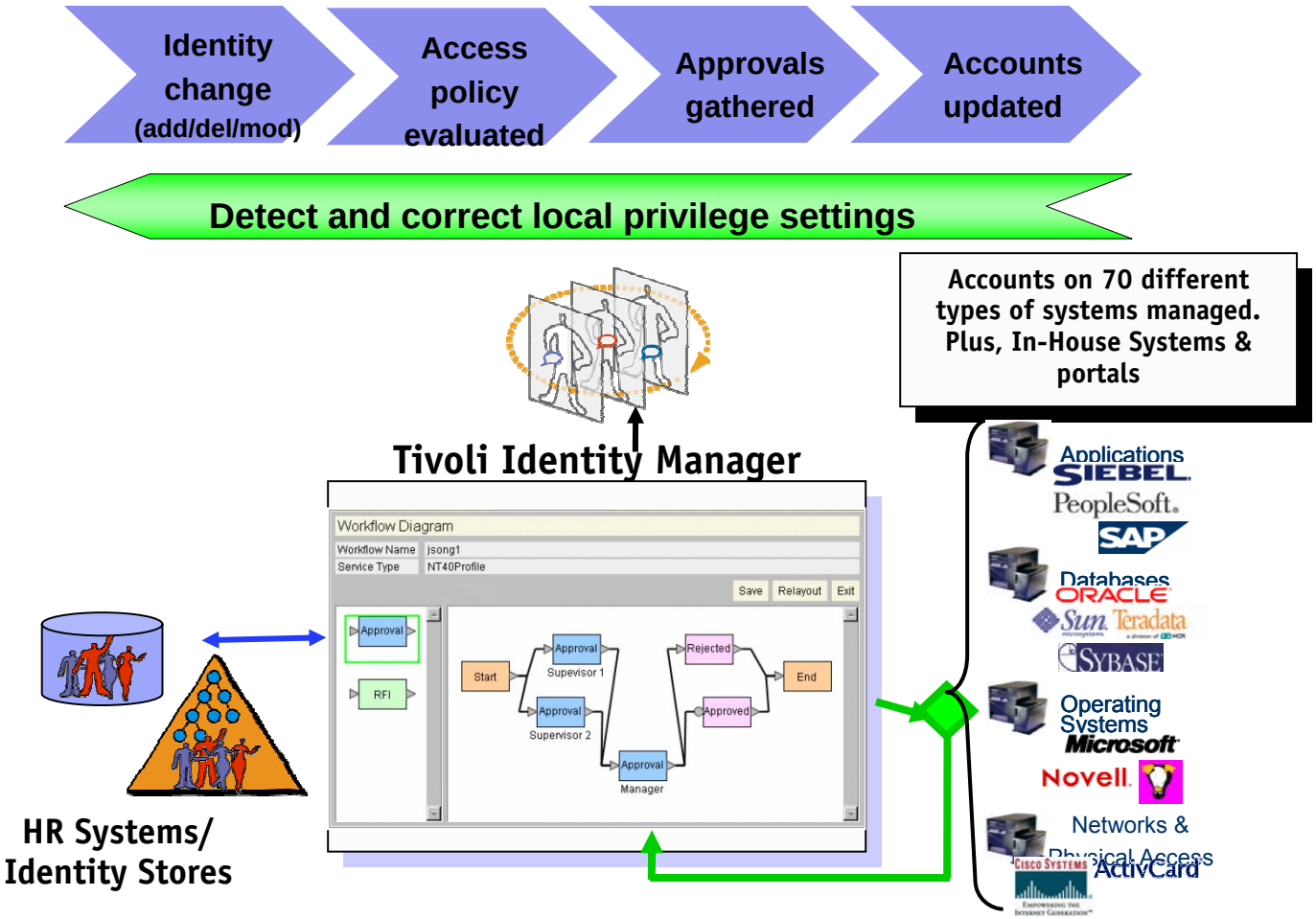
Directory Integrator - Connecting data across systems

- Moves, copies and transforms data between systems
  - Maps between schemas and attributes of the connected systems
  - The combined attribute flow and transformation rules create output for the target systems
  - Supports several scripting languages for business logic and exception handling



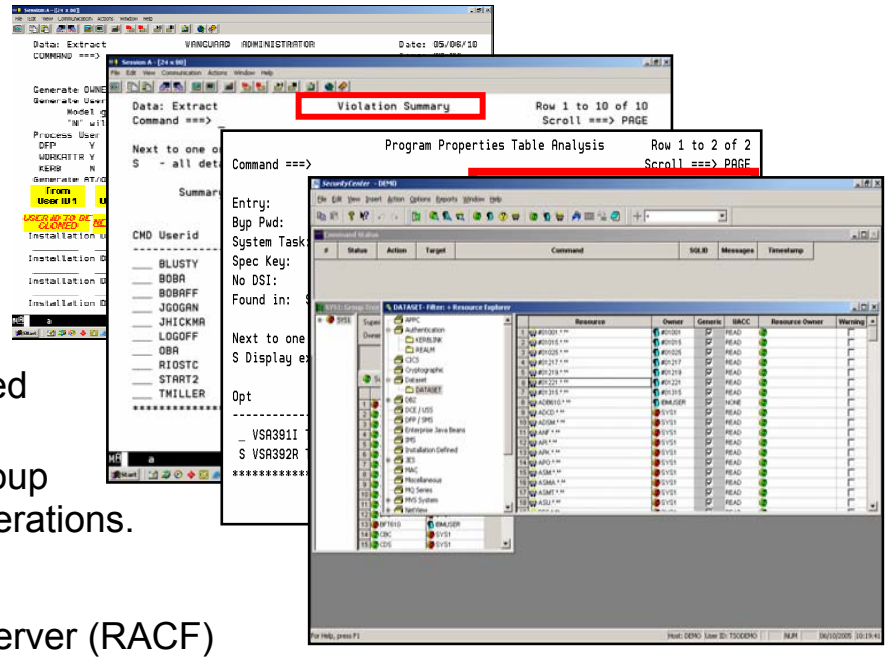
Increase speed and efficiency of security management processes with Tivoli Identity Manager

- Manage changes in minutes, not days
- Reduce errors
- Free valuable administrators for more productive work
- Support scalable business processes
- Lower help desk costs



Vanguard Tools for z/OS Augment TIM

- Vanguard Administrator
  - Robust security solution for advanced & novice RACF administrators, simplifies and enhances security management functions
  - Reduces the complexities of RACF security administration
- Vanguard SecurityCenter
  - RACF centric administration via a Windows-based graphical user interface
  - Replaces line commands with point-and-click group tree navigation, drill down and drag-and-drop operations.
- Vanguard Advisor
  - Advanced reporting tool for the z/OS Security Server (RACF)
  - Simplifies report generation with 40 pre-defined customizable reports.
- Vanguard Analyzer
  - Comprehensive auditing of the z/OS Security Server (RACF) resources
  - Includes built-in knowledge base which provides expert assistance on threats and recommended fix-actions.
- Vanguard Enforcer
  - Host-Based intrusion detection and management solution for RACF
  - Provides continuous monitoring and generates event notification.



Tivoli Access Manager Family

- TAM for Business Integration
  - Protects access to read/write to MQSeries queues
  - Protects messages sent over MQSeries queues
- TAM for Operating Systems
  - Enhances the access control checks performed by a Linux or AIX operating system
- TAM for e-business
  - Authenticates users accessing information via HTTP (web).
  - Protects access to information based on URL
  - Supports single sign on to multiple web-accessible applications
  - Protects access to EJB methods
- TAM for Enterprise Single Sign On
  - Relieves the user from answering userid/password prompts for every application
  - Can be used to set up random passwords that user does not even see or need to remember

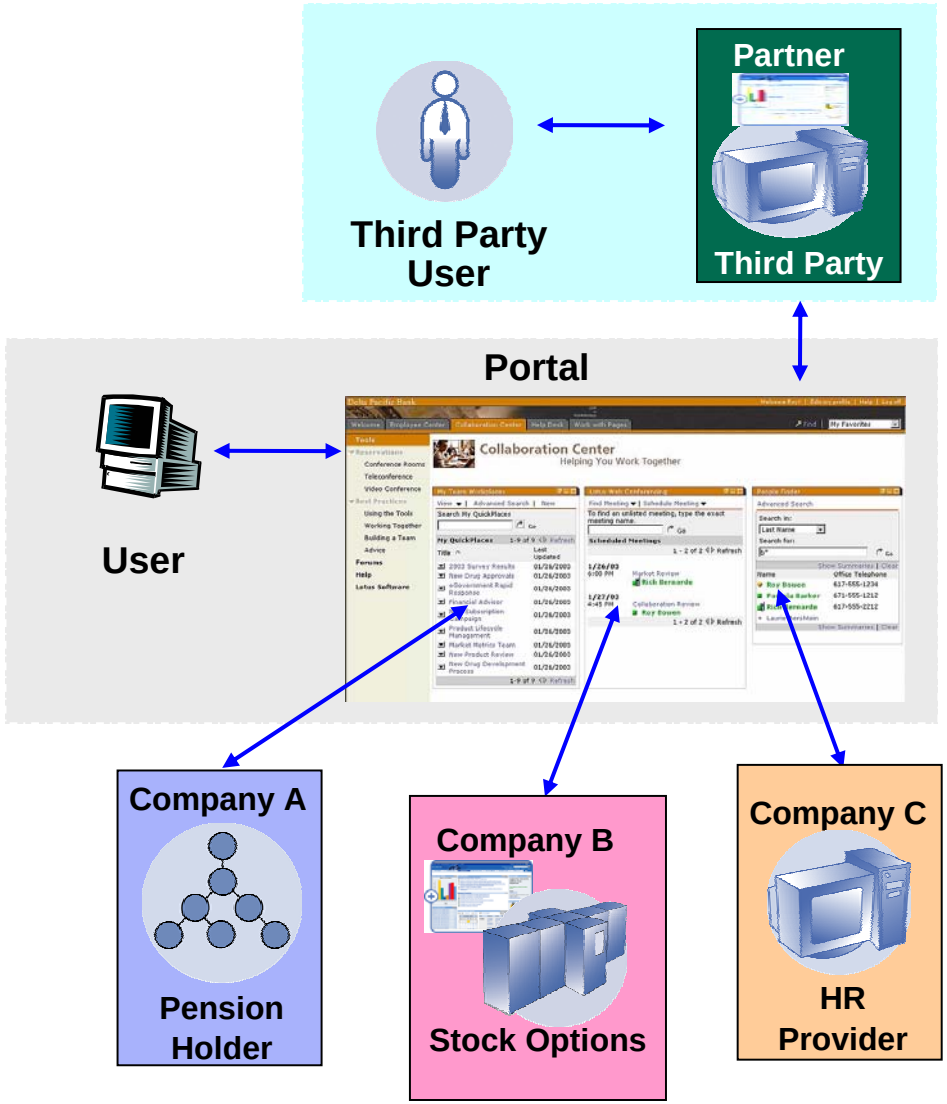
Tivoli Federated Identity Manager

Typical Scenarios

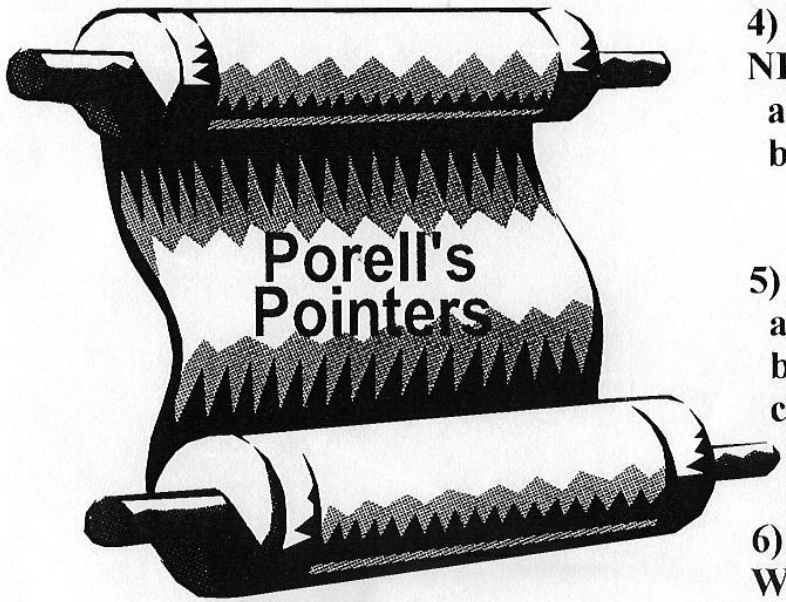
- Multiple enterprises or multiple businesses within an enterprise
- Goal: share user information among trusted partners in a transaction

Value Proposition:

- Lower identity management and help-desk costs
- Improve user experience
  - Streamlined registration
  - Federated SSO
- Enable secure, trusted business exchanges



Yea, Verily, Although I walk in a data center full of servers, I shall know no fear - for I have Porell's Pointers to guide and comfort me...



1) Look for TORTURED data flows.
Reduce the number of data moves, copies, and transforms.

2) COLLOCATE applications and data. Avoid distributed data.
 a. Distributed data may be faster to prototype, but
 b. Distributed applications will be cheaper to operate
  - Avoiding redundant security for data and applications
  - Reducing network bandwidth to move data
  - Reducing points of failure
  - Reducing two-phased commit complexity

3) Measure END-TO-END, not just one technology slice. Include performance, capital and OPERATIONS costs in measurement.

4) Understand benchmarks measure CAPITAL costs/tran of NEW systems.
 a. They assume NEW system/ server FOR EACH application.
 b. They don't include LEGACY costs used moving, copying or transforming data to NEW servers.

5) Consider INCREMENTAL growth opportunities.
 a. How many servers is enough, day 1 to year 5?
 b. How is growth satisfied, upgrade, replacement or migration?
 c. What are the hardware, software and operations growth costs?

6) Consider MULTIPLE applications and databases being WORKLOAD managed in a server at reduced operational costs.

Continued innovation in security

Almaden

- Cryptographic Foundations
- Digital Rights Management
- Privacy-Preserving Data Mining

Watson

- Cryptographic Foundations
- Network Security & "Ethical Hacking"
- Secure Embedded Systems
- Security of Autonomic Systems
- Secure Hardware
- Security Engineering
- Secure Hypervisors
- Integrity Based Computing
- Secure Linux systems & Applications High Assurance Systems
- Security Assessment Tools
- Privacy Technology
- Web Services Security
- Biometrics & Surveillance Systems

Zürich

- Cryptographic Foundations
- Java Cryptography
- Privacy Technology
- Identity Management
- Integrity-Based Computing
- Grid Computing & Web Services Security
- Intrusion Detection & Alert Correlation
- Smart Card Systems and Applications
- Java Card
- Web Services Security

Tokyo

- Web Services Security
- Mobile Security
- XML Security
- VLSI for crypto
- Digital Watermarking

On November 15th, 2005, the White House named IBM a winner of the U.S. National Medal of Technology - the highest honor awarded by the President of the United States for technology innovation

IT security

Understand, mitigate and manage security risks
IBM consulting, services and technologies