



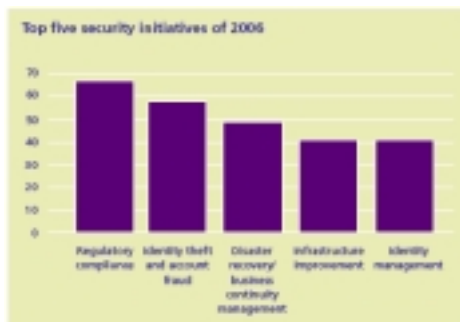
The Modern Mainframe... At the Heart of Your Business

End-to-End Security and Compliance



© 2006 IBM Corporation

Enterprise Security Has Become a Key Business Requirement



2006 Deloitte Security Survey

During the past 12 months companies reported 331 attempted and 39 successful breaches per company
- InfoWorld survey 10/20/2006

More than 1,100 Department of Commerce laptop computers were lost, stolen or missing in the last 5 years with personal data
- CNET 09-22-2006

ChoicePoint will pay \$10 M in civil penalties and \$5M million in consumer redress to settle FTC privacy charges
- FTC release 1/26/06

Service Oriented Finance Security Requirements

We have a lot of security requirements



Service Oriented Finance CIO

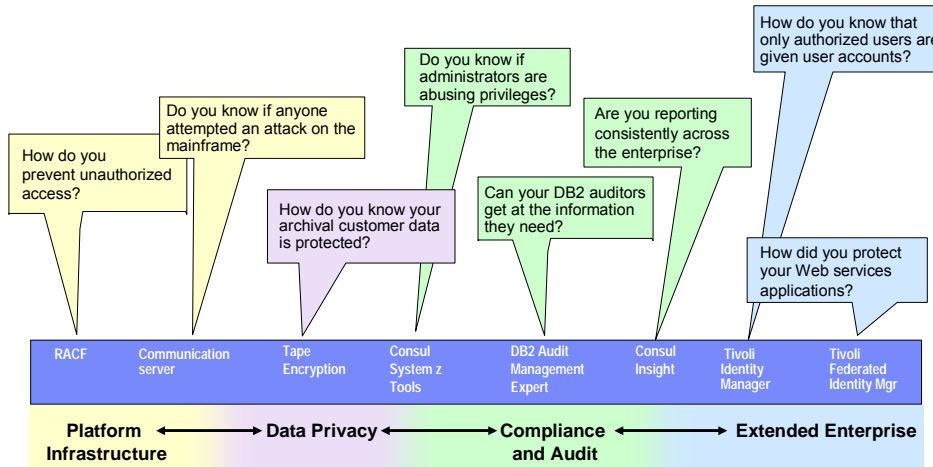
Your security strategy should include these key elements:

- Secure platform infrastructure
- Data privacy
- Compliance and audit
- Manage security across the extended enterprise

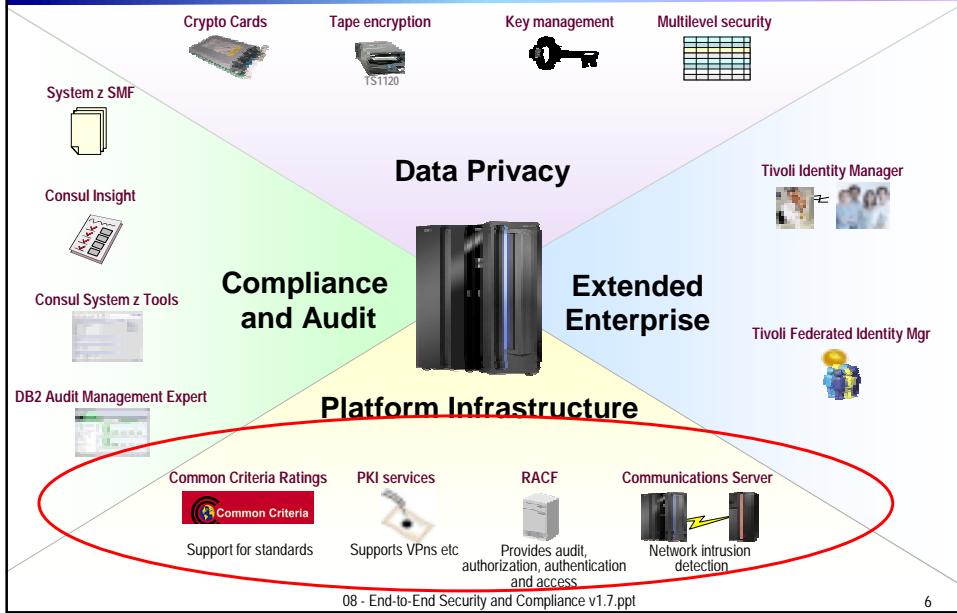


IBM

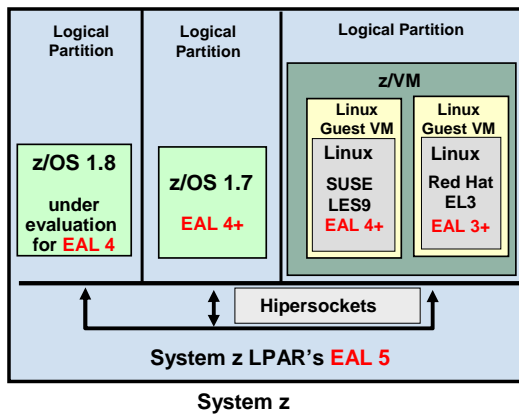
Questions Auditors Might Ask



Enterprise Security Needs Many Elements



Common Criteria Certifications Show System z Platform Security Leads the Industry



- What is Common Criteria?
 - ▶ Common Criteria is an accepted standard for evaluating the inherent security of a computing system
 - ▶ A higher EAL rating is more secure
 - ▶ The security requirements in Common Criteria have gained support as "best practices"
 - ▶ IBM System z holds the highest EAL grades in Common Criteria!
- Crypto Cards rated at FIPS 140-2 level 4

Security Begins with System z Secure Processing

- Workload Isolation
 - Isolation of users in a separate address space
 - Processing integrity with LPAR separation
 - System programs separated from user programs
- Not Harmed by Malware
 - Viruses cannot be readily introduced
- Communications
 - Internal Hipersocket communications not easily intercepted
- Authorized Program Facility (APF)
 - Executable code can be invoked only by authorized users
 - Cross memory services prevents unauthorized access
- System Integrity Statement
 - IBM accepts responsibility for integrity exposures found by customers

- System z is a hacker's nightmare!
- Allows customers to run multiple workloads on single image
- Stops viruses and worms from disrupting operations

08 - End-to-End Security and Compliance v1.7.ppt

8

RACF* – At the Heart of System z Security

- RACF controls authorization and authentication
 - ▶ Identifies and authorizes users
 - ▶ Controls access to resources
 - ▶ Authenticates users through passwords or (PKI) digital certificates
 - ▶ Provides auditing and logging
 - ▶ Enables central administration of several systems
- RACF structure is enforced automatically
 - ▶ System blocks unauthorized attempts
 - ▶ You cannot bypass RACF
- RACF is integrated with System z Middleware
 - ▶ Transaction monitors, DB2
 - ▶ CICS, IMS, WebSphere

These resources are protected by RACF

- | | |
|---------|-------------|
| ▶ DB2 | ▶ JES 2 & 3 |
| ▶ VSAM | ▶ Console |
| ▶ IMS | ▶ VTAM |
| ▶ CICS | ▶ SDSF |
| ▶ TSO | ▶ WebSphere |
| ▶ Disk | ▶ MQ |
| ▶ Tape | ▶ Programs |
| ▶ Print | ▶ Keys |

Integrated Security across the platform

* Resource Access Control Facility

08 - End-to-End Security and Compliance v1.7.ppt

9

Authenticate at Low Cost with Digital Certificate Services

Banco do Brasil saves an estimated **\$16 M** a year in digital certificate costs by using the digital certificate services offered free with System z

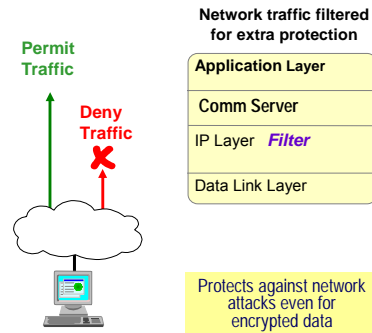
- A digital certificate is an electronic identifier that establishes your credentials on the Web
- Recently digital certificate use has grown to help meet compliance requirements
- z/OS automatically provides support for digital certificate services (PKI)
- Uses System z cryptographic processor
 - ▶ No need for extra infrastructure
 - ▶ Processes thousands of certificates at low cost
- The mainframe can serve as a certificate authority - an authority that manages provisioning of digital certificates.
 - ▶ This eliminates fees to third parties (\$5 - \$7 per certificate) for issuing certificates

08 - End-to-End Security and Compliance v1.7.ppt

10

Built in Security to Defend Against Network Attacks

- **Intrusion Detection** from Communications Server enables detection of network traffic attacks
- Automatic application of defensive mechanisms
 - ▶ Evaluates inbound encrypted data for suspect activity
 - ▶ Policy controls connection limits, packet discard
 - ▶ Detects anomalies in *real-time*
 - ▶ Avoids *overhead* of per packet evaluation against known attacks
- Scan detection and reporting
 - ▶ Can map the target of an attempted attack
- Integrates with Tivoli Security Operations Manager

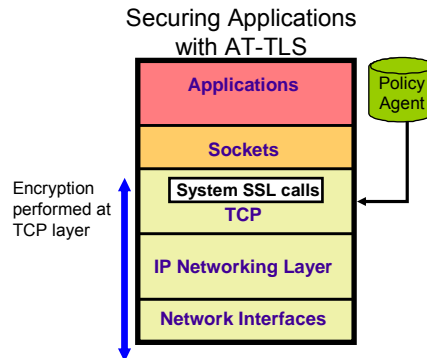


08 - End-to-End Security and Compliance v1.7.ppt

11

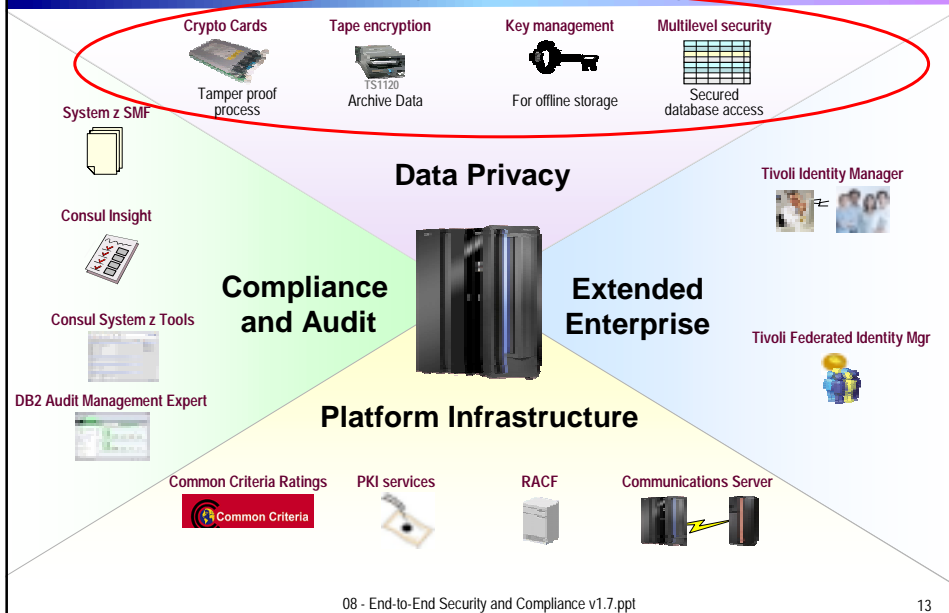
Provide Cryptographic Protection without Changing Application Code

- Application Transparent Transport Layer Security TLS * provides cryptographic protection between clients and servers
- Configure encryption via the communication server
- Application can also issue AT-TLS calls to receive user identity information based on client certificate
- AT-TLS uses an optimized infrastructure that outperforms native SSL/TLS



*Transport Layer Security (TLS) is based on Secure Socket Layer

Enterprise Security Needs Many Elements



The Foundation of Data Privacy is Encryption

Free - CP Assist for Cryptographic Function (CPACF)

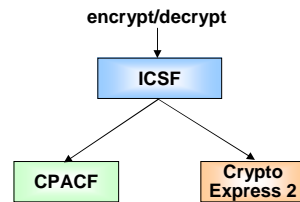
- Each system processor has hardware assist on the chip for cryptography
- CPACF provides cryptographic functions for encryption and decryption of data
 - ▶ Used for SSL, VPN, and data storing applications
 - ▶ includes DES, T-DES, AES, SHA-1 and SHA-256 hashing

Priced Feature - Crypto Hardware Processor Card

- Crypto Express 2 (\$38K per card)
- High performance, tamper proof environment for secure key cryptography
- 6000 Secure Socket Layer handshakes per second
- Key is encrypted in hardware and never exposed

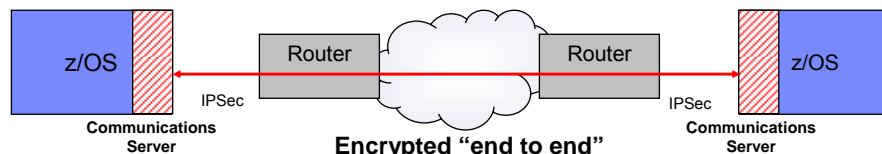
Integrated Cryptographic Service Facility (ICSF)

- Provides API's for encryption via CPACF or Crypto Express2
- Routes work to the appropriate crypto processing resource
- Included in z/OS
- Used to administer the cryptographic hardware and keys



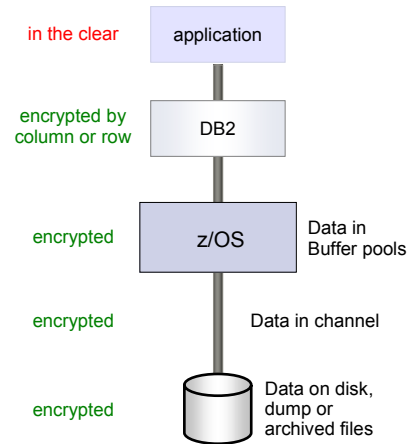
Encryption Protects Data Privacy on the Network

- End to end network encryption is needed to meet Payment Card Industry requirements
- System z Communication Server uses crypto express 2 to encrypt network data end-to-end
 - ▶ Supports IPSec protocol for virtual private networks across the internet
- New support for encrypting data on the mainframe *before sending to printers*
 - ▶ IPSec support installed in new printers
 - ▶ LAN printers can now print confidential material on secured printers
- Router based encryption is not enough
 - ▶ May expose data in the clear



DB2 Encryption Protects Data Privacy in the Database

- Encrypted by DB2
 - ▶ Table and Index encryption
 - ▶ Image copies encrypted
 - ▶ Logs/archives encrypted
 - ▶ Data encrypted in buffers
 - ▶ Data sent by DRDA
 - ▶ Data not exposed!
- DB2 uses encryption to protect the data:
 - ▶ Column level encryption
 - Enabled by the application
 - ▶ Row level encryption
 - IBM Encryption Tool for DB2
 - Optional feature

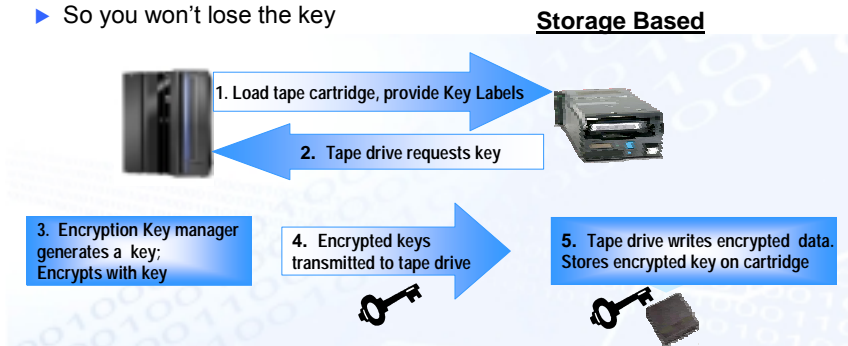


08 - End-to-End Security and Compliance v1.7.ppt

16

Optional Ability to Automatically Encrypt All Data on Tape

- High performance tape encryption
 - ▶ Standard feature on all new TS1120 Tape Drives
 - ▶ Cost effectively encrypt all tape data
 - ▶ Offload host processing encryption overhead
 - ▶ Minimize impact to existing processes and applications
- Leverages System z Key management
 - ▶ So you won't lose the key



08 - End-to-End Security and Compliance v1.7.ppt

17

Keep Your Key Safe with System z Key Management

Encryption Key Manager (EKM)

- Transparently generates, serves, stores, and retrieves keys
 - ▶ Included in z/OS

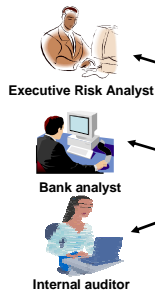
- Helps protect and manage keys
 - ▶ Generate and serves keys to tape drives
 - ▶ Utilizes tamper-resistant crypto cards to store “secure keys”
 - ▶ Obtains the required keys from key stores through Integrated Cryptographic Service Facility (ICSF)

- Provides a single point of control
 - ▶ Simplified recovery of keys
 - ▶ Auditable through RACF
 - ▶ Leverages security of System z
 - ▶ Over a decade of proven production use
 - ▶ Available at no additional charge

DB2 Multi Level Security

Goals of Compartmentalized Data

- Same database used by organizations with a different need to know
- Prevent unauthorized individuals from accessing information at a higher classification than authorized
- Prevent unauthorized declassification of information



| SECURITY Classification | Revenue | Area | Loss |
|-------------------------|---------|----------|------|
| Executive | 234 | USA | 3% |
| Finance Secret | 198 | Ohio | 13% |
| Executive | 2 | Maine | 29% |
| Finance Confidential | 234 | USA | 11% |
| Finance Secured | 87 | Texas | 14% |
| Finance Secured | 23 | New York | 20% |
| Audit Confidential | 223 | USA | 10% |
| Finance Secured | 45 | Canada | 29% |

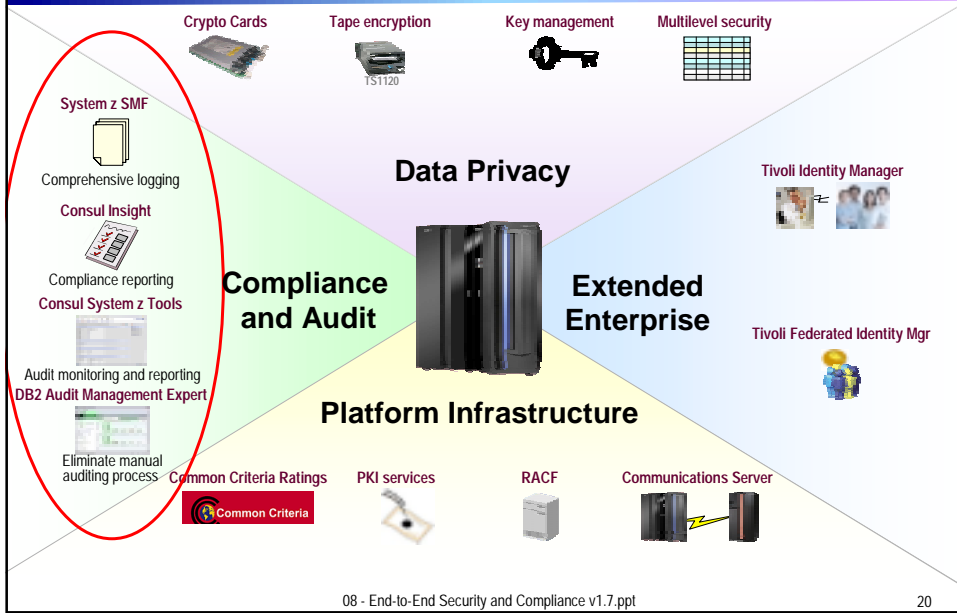
Single image of data is sharable by multiple enterprise departments with different levels of “need to know”

DB2 Multi Level Security

- Restricts row level access to those with appropriate security clearance
- Mix low and high security data in the same database

With DB2 Multi Level Security data can be consolidated onto a single database, restricting access to only authorized users

Enterprise Security Needs Many Elements



Evolving Regulations Point to the Need for More Automated Compliance Reporting

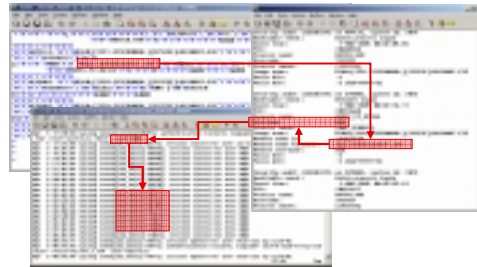
| | Regulatory Impact | | | | | |
|---------------------------|-------------------|----------|-----------|-----------------|----------------|----------------------------|
| | Secured Data | Workflow | Reporting | Risk Assessment | Encrypted data | Secured Storage Management |
| Basel II | ✓ | ✓ | ✓ | ✓ | ✓ | |
| HIPAA | ✓ | ✓ | ✓ | | ✓ | ✓ |
| Sarbanes-Oxley | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Gramm Leach-Bliley | ✓ | | ✓ | | | |
| AML - Patriot Act | ✓ | | ✓ | | ✓ | |

IBM Service Management Market Needs Study, March 2006

The Foundation of Audit and Compliance is Comprehensive Logging

- System z SMF provides comprehensive logging across the sysplex
 - ▶ Consistent record formats help simplify compliance needs
 - ▶ Audit records report access to protected resources
- New *log continuity* from Consul validates logs have been maintained
 - ▶ Consul uses the log system event records from multiple sources including System z
 - ▶ Can examine activities of a specific user

With distributed systems, customers have to manually piece together logs



08 - End-to-End Security and Compliance v1.7.ppt

22

Consul InSight Strengthens the Compliance Process

- **Detects** security violations
- **Captures** security audit data from multiple systems
- **Correlates** data to identify audit risks
 - ▶ who, what, on what, where, when, from where, to where
- **Analysis engine** for deep analysis of collected data
 - ▶ Determine who was the last person to touch a particular file
- **Flexible reporting** related to specific compliance issues
- Checks for **log continuity** ensure that log collection is carried out

08 - End-to-End Security and Compliance v1.7.ppt

23

DEMO: Consul InSight

Consul InSight detected that our employee Michael, has been accessing restricted data.

How did this happen?



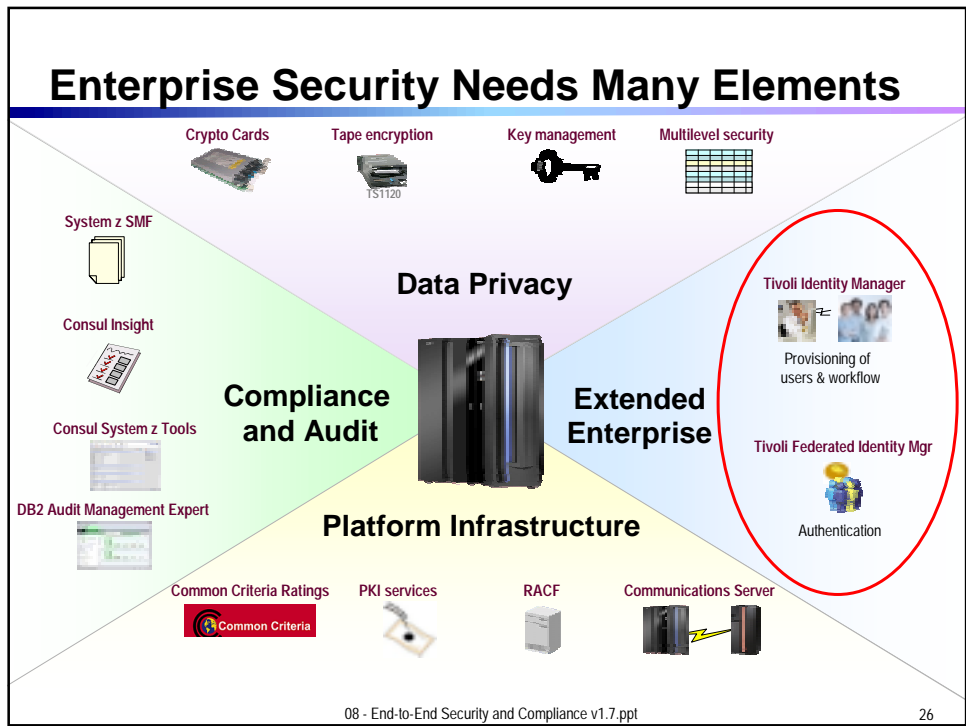
Service Oriented Finance
Security Officer



Other Consul Products Supports System z Auditing and Security Monitoring

Consul tools interoperate to improve auditing and forensic capabilities

- **zAudit** is an audit and reporting tool for the mainframe environment
 - ▶ Built-in knowledge base identifies exposures
 - ▶ Provides real-time alerts based on policy exceptions
- **zAlert** provides real-time threat monitoring for z/OS and RACF
 - ▶ Can issue alerts when conditions occur
 - ▶ Can take action to stop security breaches
- **zLock** prevents erroneous commands, thereby increasing control and decreasing the security risk and clean-up cost
 - ▶ Prevent non-compliant RACF commands from executing
 - ▶ Reduce security risks due to improper administration
- Flexible **CARLa** (Consul Audit and Reporting Language) language for customized user reporting



Provision Users with Tivoli Identity Manager for z/OS

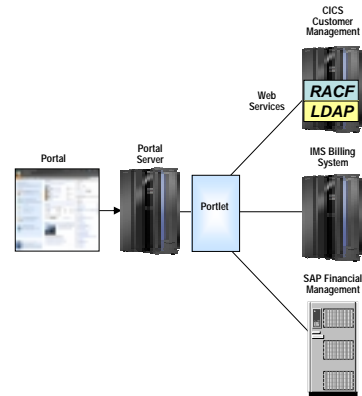
- 75-80% of help desk calls are for password reset or other trivial items
- Tivoli Identity Manager can eliminate this problem
- Provides self service password management
- Can provision user accounts for your entire enterprise

- Provides workflow for automating approval processes
- Searches for out-of-policy changes
- Provides email notification of changes

08 - End-to-End Security and Compliance v1.7.ppt 27

Single Sign-on: Tivoli Federated Identity Manager

- Propagates the identity of the original requester in a **web services** environment
 - ▶ Provides single sign-on for web services
 - ▶ Maintains identity of the original user
 - ▶ Credentials can be propagated from the portal to RACF for end-to-end security
 - Uses Passtickets issued by RACF
 - ▶ Enable trusted transactions between business partners
 - ▶ Supports industry standards
 - SAML, Liberty, WS-Federation SSO



TFIM can provide single sign-on for the Service Oriented Finance Car Loan Solution

Service Oriented Finance Requirements Met

So do you feel more secure?



IBM

My systems are now secure with System z

- Secure platform infrastructure!
- Data privacy!
- Compliance and audit!
- Security across the extended enterprise!



Service Oriented Finance
CIO

