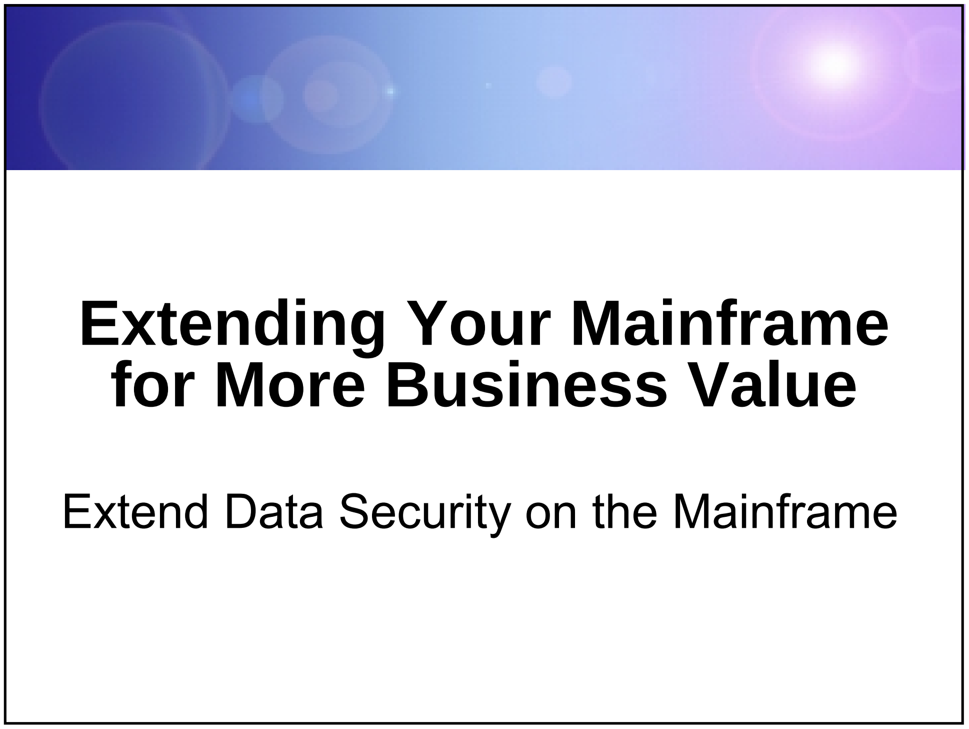
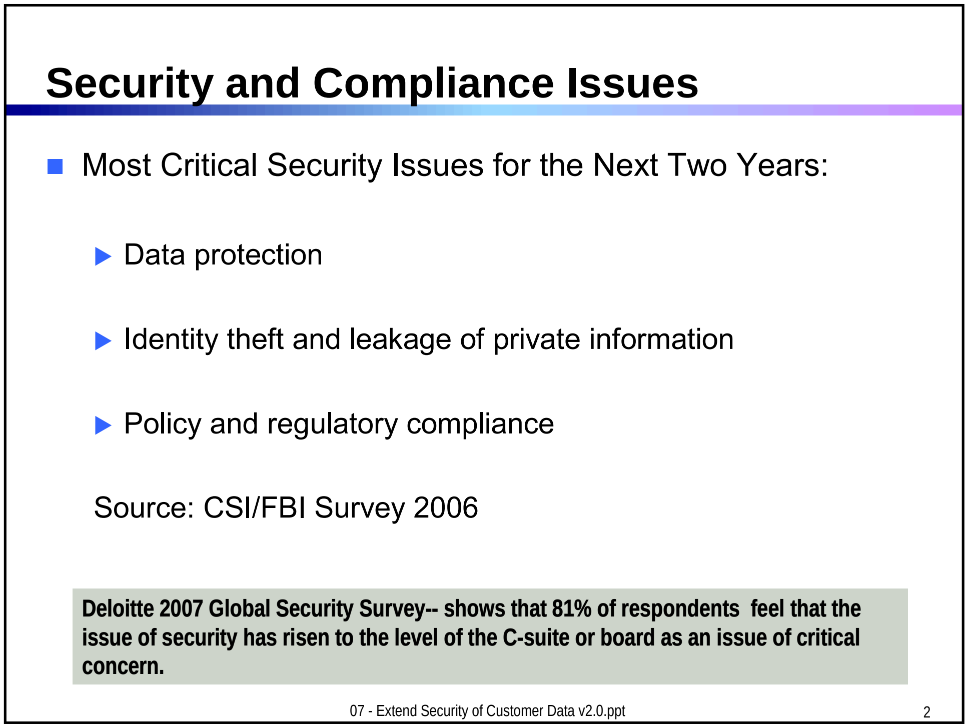


Extending Your Mainframe for More Business Value

Extend Data Security on the Mainframe

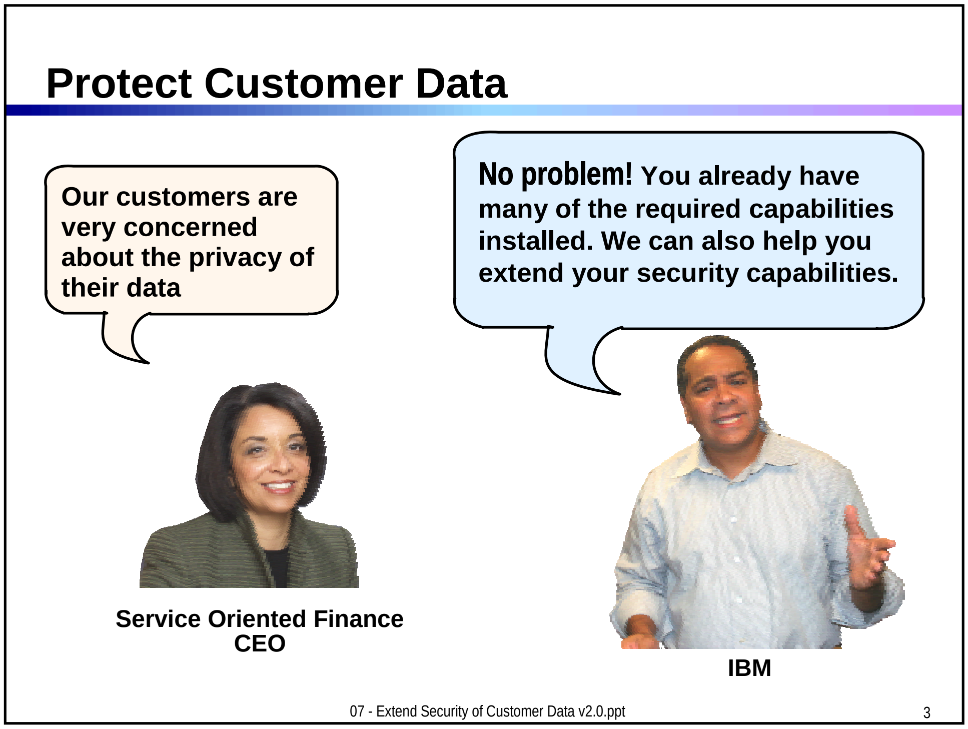


Security and Compliance Issues

- Most Critical Security Issues for the Next Two Years:
  - Data protection
  - Identity theft and leakage of private information
  - Policy and regulatory compliance

Source: CSI/FBI Survey 2006

Deloitte 2007 Global Security Survey-- shows that 81% of respondents feel that the issue of security has risen to the level of the C-suite or board as an issue of critical concern.



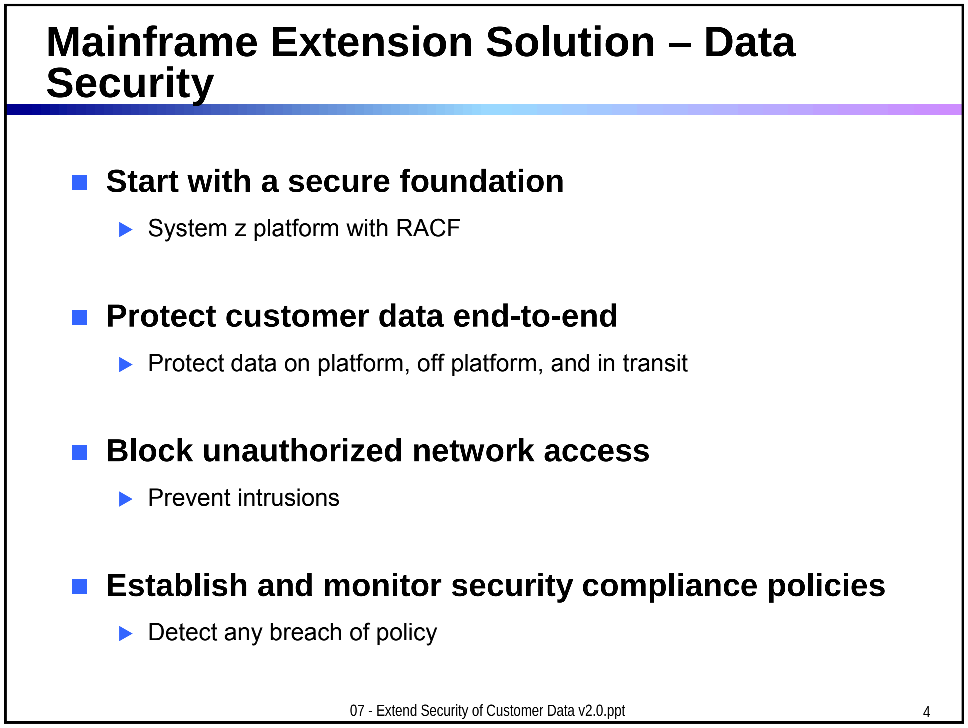
Protect Customer Data

Our customers are very concerned about the privacy of their data

No problem! You already have many of the required capabilities installed. We can also help you extend your security capabilities.

Service Oriented Finance CEO

IBM



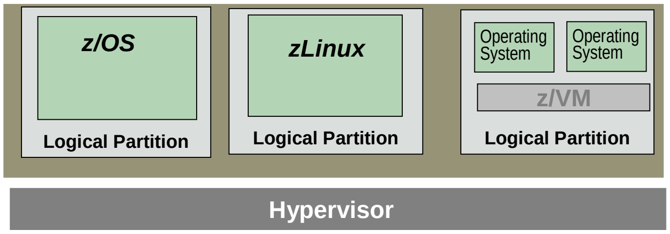
Mainframe Extension Solution – Data Security

- **Start with a secure foundation**
  - System z platform with RACF
- **Protect customer data end-to-end**
  - Protect data on platform, off platform, and in transit
- **Block unauthorized network access**
  - Prevent intrusions
- **Establish and monitor security compliance policies**
  - Detect any breach of policy

A Secure Foundation is a Prerequisite to Address Security Issues

- **Workload Isolation**
  - System z Hypervisor maintains strict isolation between workloads
  - Hardware coded storage protect keys protects system and user workloads
  - Architecture design makes typical buffer overflows and virus payloads inoperable
  - HiperSockets provides secure internal communications
- **Integrated access control throughout the stack**
  - RACF enforces access control and logs security events
- **Secure cryptographic encoding**
  - On chip crypto hardware assist and optional high speed cryptographic processors
  - Key management facility

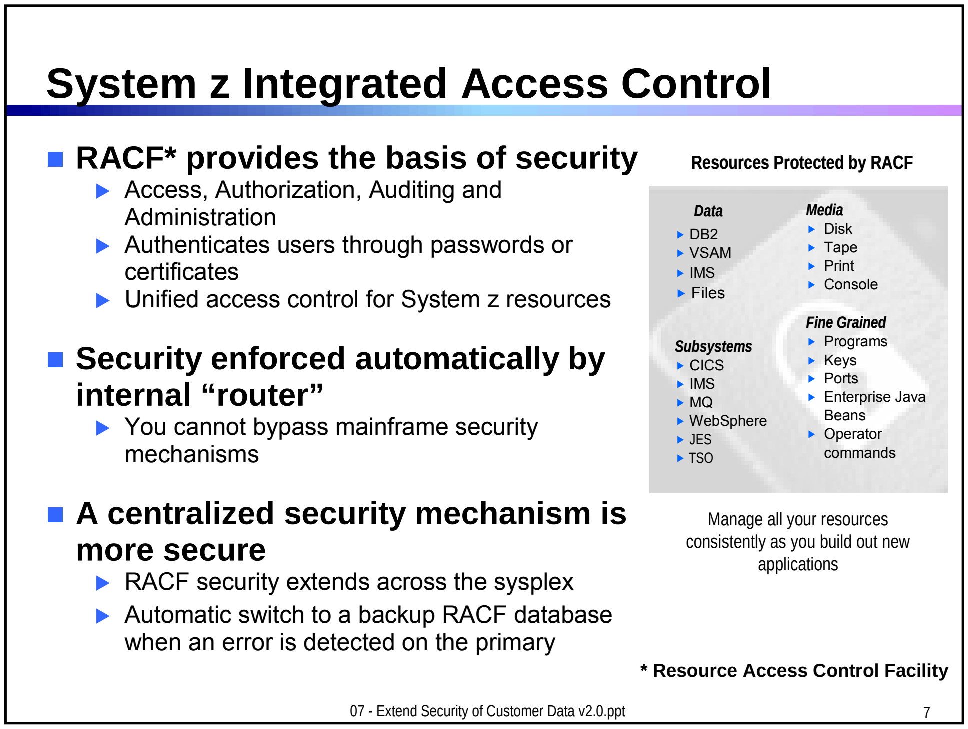
A Secure Foundation Requires The Highest Common Criteria Rating for Security



Partition Manager	Linux	Other OS	VM	DB2
EAL5+	EAL4 for SuSE and Red Hat	z/OS EAL4	zVM EAL3	DB2 for z/OS In Evaluation @ EAL3

Highest Ratings

- Common Criteria is an accepted standard for evaluating the security of a computing system
- IBM System z holds the **highest** commercial operating system EAL (Evaluation Assurance Level) ratings at 5+
- System z prevents unauthorized information flow between logical partitions so that confidential data remains protected



System z Integrated Access Control

- **RACF* provides the basis of security**
  - Access, Authorization, Auditing and Administration
  - Authenticates users through passwords or certificates
  - Unified access control for System z resources
- **Security enforced automatically by internal "router"**
  - You cannot bypass mainframe security mechanisms
- **A centralized security mechanism is more secure**
  - RACF security extends across the sysplex
  - Automatic switch to a backup RACF database when an error is detected on the primary

Resources Protected by RACF

Data
- DB2
- VSAM
- IMS
- Files

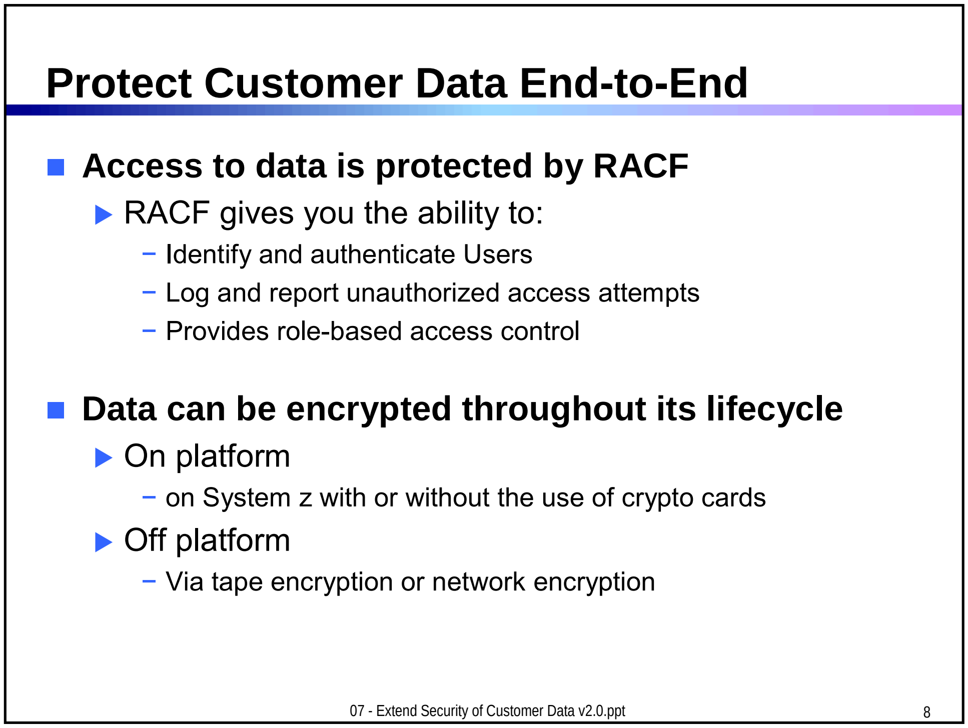
Media
- Disk
- Tape
- Print
- Console

Subsystems
- CICS
- IMS
- MQ
- WebSphere
- JES
- TSO

Fine Grained
- Programs
- Keys
- Ports
- Enterprise Java Beans
- Operator commands

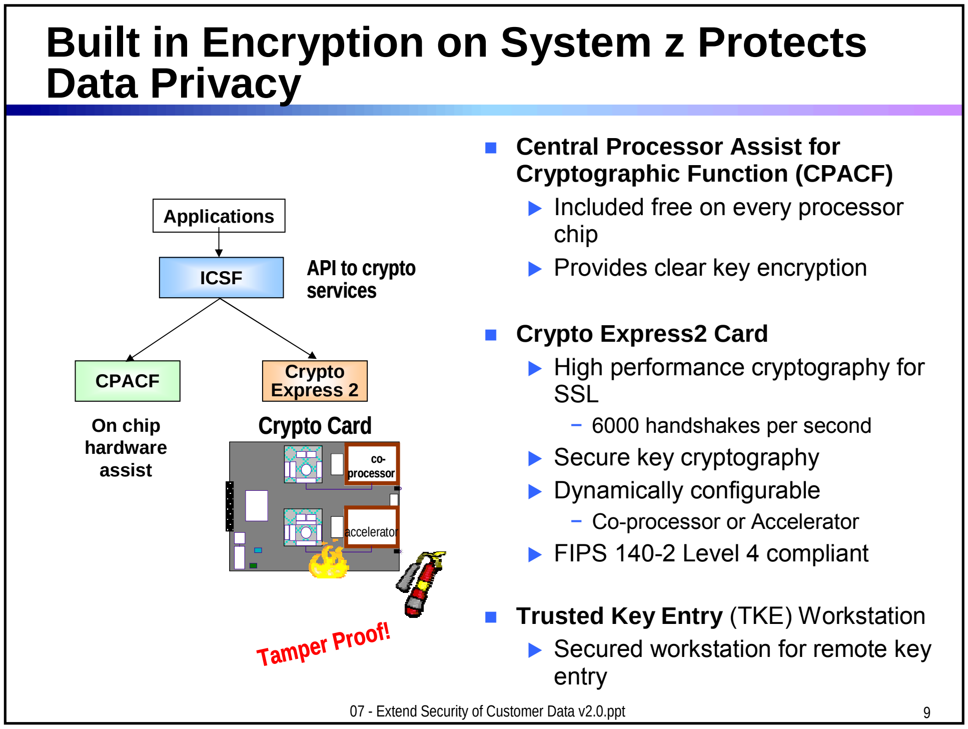
Manage all your resources consistently as you build out new applications

*** Resource Access Control Facility**



Protect Customer Data End-to-End

- **Access to data is protected by RACF**
  - RACF gives you the ability to:
    - Identify and authenticate Users
    - Log and report unauthorized access attempts
    - Provides role-based access control
- **Data can be encrypted throughout its lifecycle**
  - On platform
    - on System z with or without the use of crypto cards
  - Off platform
    - Via tape encryption or network encryption



Built in Encryption on System z Protects Data Privacy

Applications

ICSF

API to crypto services

CPACF

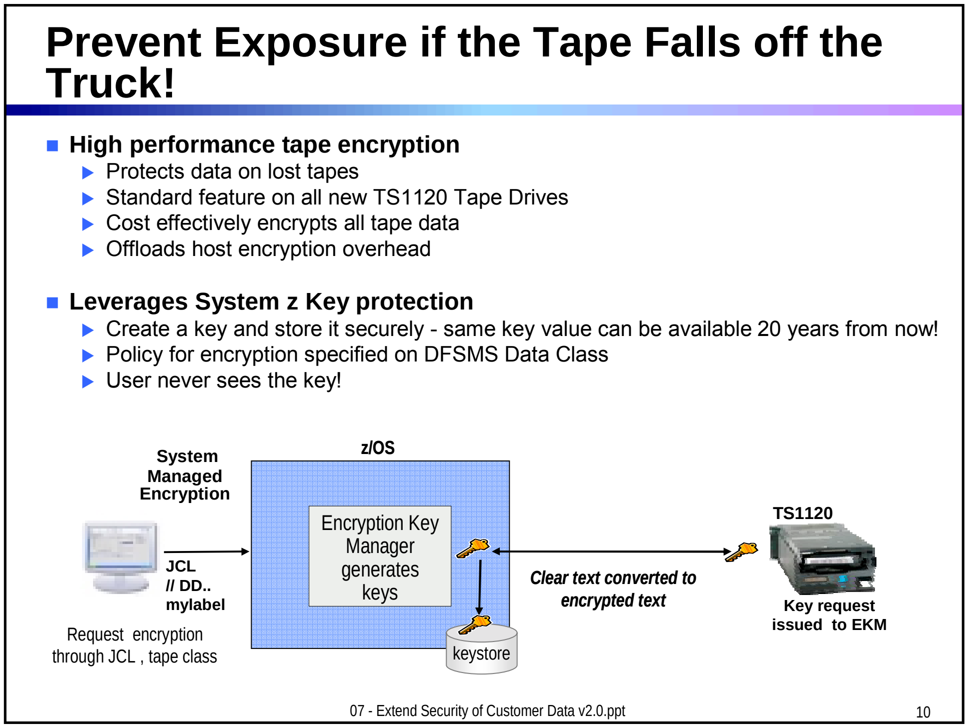
On chip hardware assist

Crypto Express 2

Crypto Card

Tamper Proof!

- **Central Processor Assist for Cryptographic Function (CPACF)**
  - Included free on every processor chip
  - Provides clear key encryption
- **Crypto Express2 Card**
  - High performance cryptography for SSL
    - 6000 handshakes per second
  - Secure key cryptography
  - Dynamically configurable
    - Co-processor or Accelerator
  - FIPS 140-2 Level 4 compliant
- **Trusted Key Entry** (TKE) Workstation
  - Secured workstation for remote key entry



Prevent Exposure if the Tape Falls off the Truck!

- **High performance tape encryption**
  - Protects data on lost tapes
  - Standard feature on all new TS1120 Tape Drives
  - Cost effectively encrypts all tape data
  - Offloads host encryption overhead
- **Leverages System z Key protection**
  - Create a key and store it securely - same key value can be available 20 years from now!
  - Policy for encryption specified on DFSMS Data Class
  - User never sees the key!

System Managed Encryption

z/OS

Encryption Key Manager generates keys

keystore

JCL
// DD..
mylabel

Request encryption through JCL , tape class

Clear text converted to encrypted text

TS1120

Key request issued to EKM

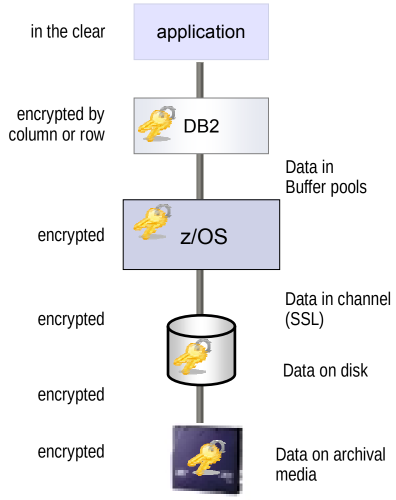
System z Encryption Key Management

Encryption Key Manager (EKM)

- Java program that transparently generates, serves and maintains encryption keys
- **Provides a single point of control**
  - Simplified recovery of keys
  - Auditable through RACF
  - Over a decade of proven production use
  - Available at no additional charge
- **Helps protect and manage keys**
  - Generate and serves keys to tape drives
  - Uses tamper-resistant crypto cards to store “secure keys”
  - Can retrieve required keys from protected key stores
- **Options to store the keys**:
  - RACF protected key stores
  - Secure hardware
  - Other protected data sets, files

Protect Data Privacy Using DB2

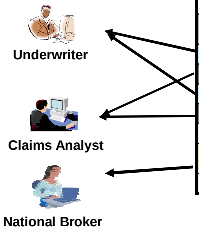
- DB2 uses either clear key (CPACF) or secure key (Crypto Express2 card) for encryption
- DB2 supports encryption at every level:
  - In memory, buffers, disk, and archival media
  - Table, Index, logs, and backup copies
  - Data sent by remote access (DRDA)
- DB2 provides multiple options for table encryption:
  - Column level encryption
    - Enabled by the application
  - Row level encryption
    - IBM Encryption Tool for DB2



Multi-Level Security (MLS) Supports Users with Different Security Clearances

Goals of Multi-Level Security

- Share one data base among organizations with different “need to know”
- Prevent individuals from accessing information at a higher classification level than what is permitted
- Prevent unauthorized *declassification* of information to a lower classification level than at which it was accessed (“Write-down”)



SECURITY Classification	Revenue	Area	Loss
Business Broker	234	USA	50%
Underwriter	198	Ohio	23%
Claims analyst	2	Maine	9%
Underwriter	234	USA	11%
Claims analyst	87	Texas	14%
Affiliate broker	23	NewYork	20%
National broker	223	USA	10%
Affiliate broker	45	Canada	29%

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

DB2 Multi-Level Security

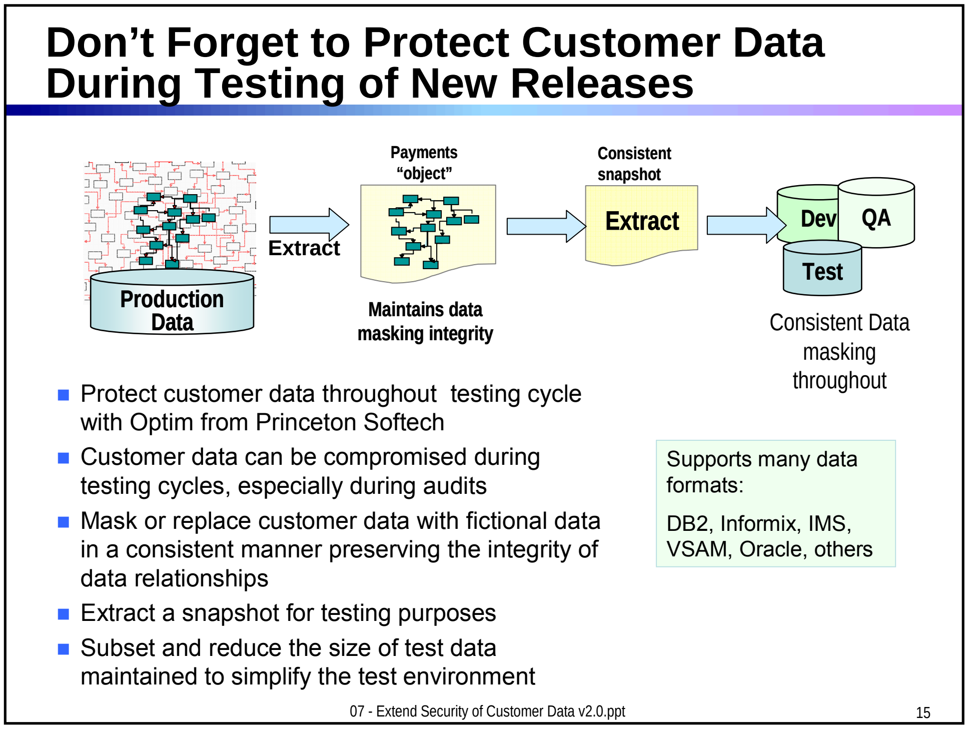
- DB2 row level security
- Restricts row level access to those with appropriate clearance
- Combines both low and high security data in the same database-eliminating redundant infrastructures

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

Abraxas Informatik Uses RACF for Secure Outsourcing Services

- Abraxas Informatik AG is one of the largest governmental outsourcers in Switzerland
- Challenges Abraxas faced:
  - High levels of security were needed to handle confidential government information
  - Both CA ACF2 and Top Secret were installed, requiring staff knowledgeable in both
  - Abraxas needed to simplify their security structure, and reduce security expenses without jeopardizing security
- Solution:
  - RACF allowed Abraxas to quickly manage resource access and user accountability while reducing costs
- Results:
  - Abraxas now saves 200,000 Swiss francs or $US 180,042 annually
  - Abraxas is now better positioned to offer excellent security services while keeping its fees competitive

abraxas Informatik AG
Ihr Informatik-Partner für öffentliche Verwaltungen und Organisationen

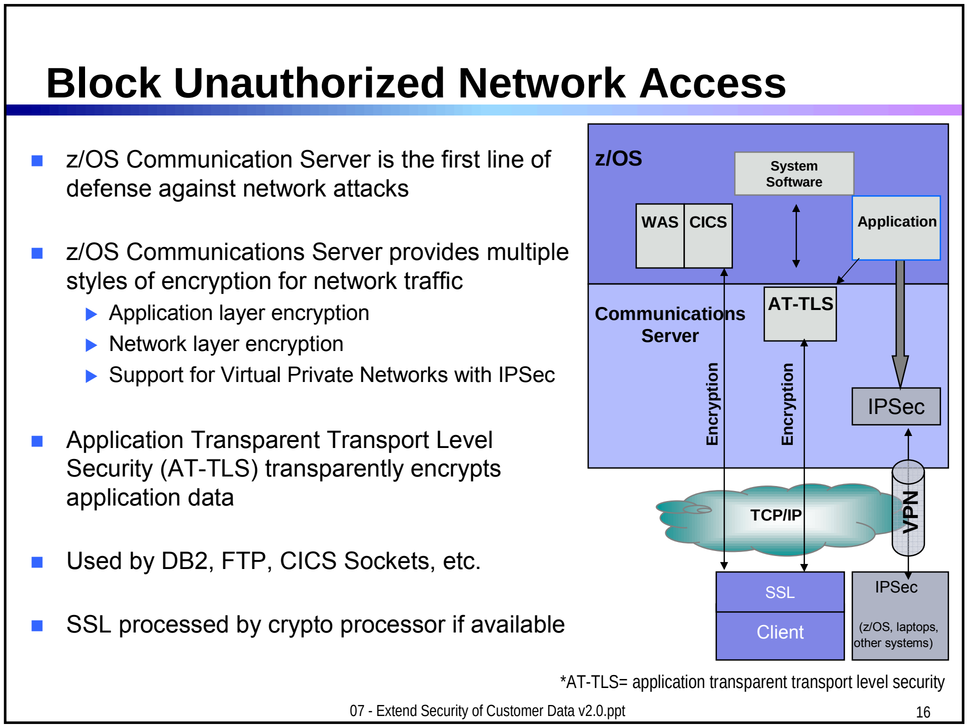


Don’t Forget to Protect Customer Data During Testing of New Releases

- Protect customer data throughout testing cycle with Optim from Princeton Softech
- Customer data can be compromised during testing cycles, especially during audits
- Mask or replace customer data with fictional data in a consistent manner preserving the integrity of data relationships
- Extract a snapshot for testing purposes
- Subset and reduce the size of test data maintained to simplify the test environment

Supports many data formats:

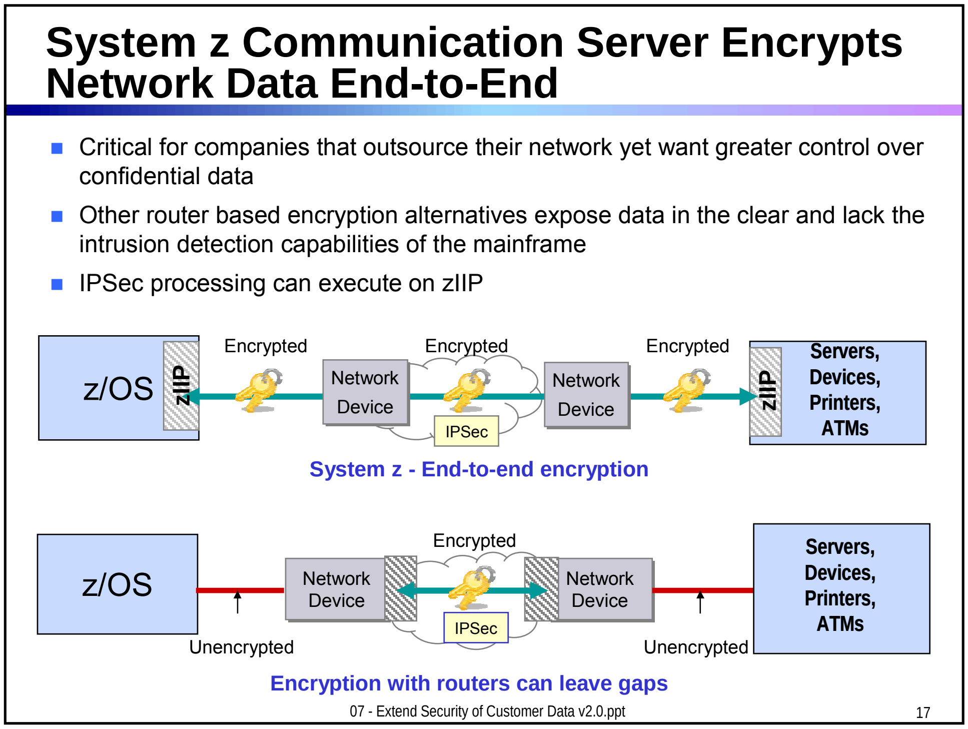
DB2, Informix, IMS, VSAM, Oracle, others



Block Unauthorized Network Access

- z/OS Communication Server is the first line of defense against network attacks
- z/OS Communications Server provides multiple styles of encryption for network traffic
  - Application layer encryption
  - Network layer encryption
  - Support for Virtual Private Networks with IPSec
- Application Transparent Transport Level Security (AT-TLS) transparently encrypts application data
- Used by DB2, FTP, CICS Sockets, etc.
- SSL processed by crypto processor if available

*AT-TLS= application transparent transport level security

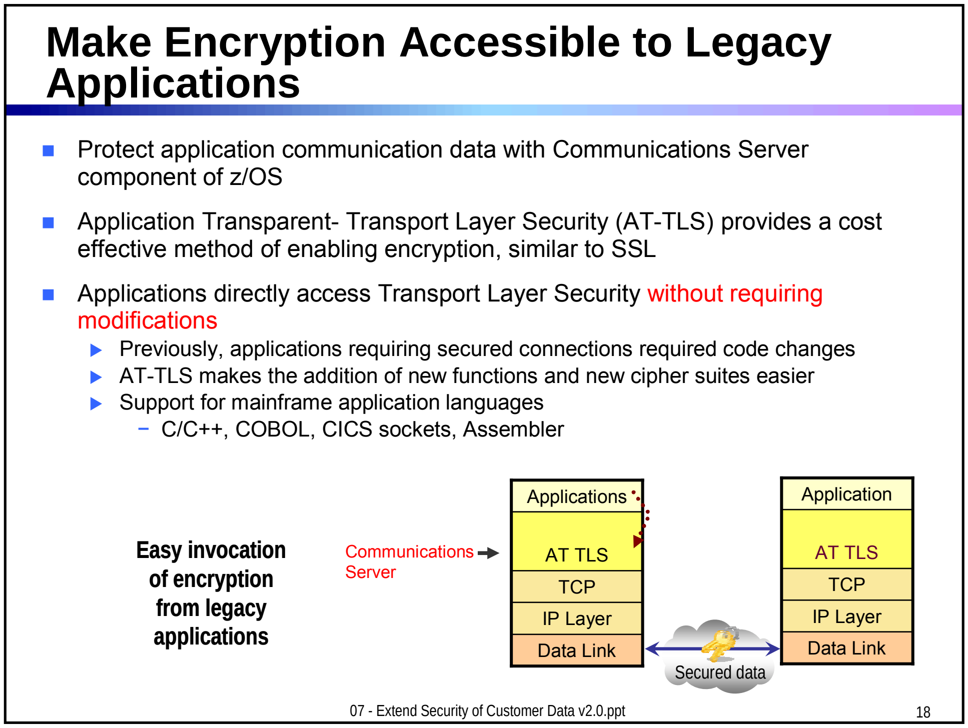


System z Communication Server Encrypts Network Data End-to-End

- Critical for companies that outsource their network yet want greater control over confidential data
- Other router based encryption alternatives expose data in the clear and lack the intrusion detection capabilities of the mainframe
- IPSec processing can execute on zIIP

System z - End-to-end encryption

Encryption with routers can leave gaps



Make Encryption Accessible to Legacy Applications

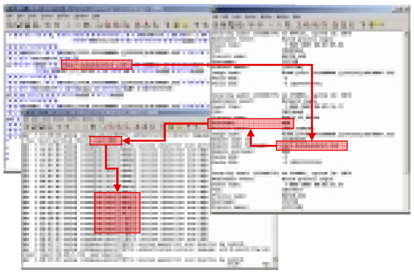
- Protect application communication data with Communications Server component of z/OS
- Application Transparent- Transport Layer Security (AT-TLS) provides a cost effective method of enabling encryption, similar to SSL
- Applications directly access Transport Layer Security without requiring modifications
  - Previously, applications requiring secured connections required code changes
  - AT-TLS makes the addition of new functions and new cipher suites easier
  - Support for mainframe application languages
    - C/C++, COBOL, CICS sockets, Assembler

Easy invocation of encryption from legacy applications

Establish And Monitor Security Compliance Policies

- The mainframe offers comprehensive built in auditing capabilities for all its subsystems
  - Unified access control with RACF
  - Common logging of RACF security events
- Enables the monitoring of users and their activities
  - Report on attempts to perform unauthorized actions
  - RACF cuts SMF (Systems Management Facility) type 80 records for post processing
  - SMF Data Unload Utility creates XML output
- System z’s common approach to log processing avoids extra integration and compliance challenges posed by inconsistent and incompatible log formats

With other systems, customers have to manually make sense out of all these different log formats

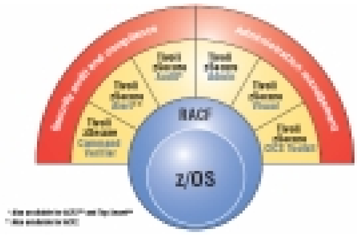


RACF Security Event Logging

- RACF helps you to audit access control and accountability:
  - Started during IPL to prevent vulnerabilities from being introduced
  - Audit control functions specify the information RACF should log
  - SMF datasets themselves are protected
  - RACF SMF data unload utility converts SMF records into a format used by other tools
- RACF logs many events:
  - All accesses to specific data sets, general resources
  - All accesses to a specified class of resources at a specified access level
  - All attempts to access a resource with a security level of confidential
  - RACF-related activities of specific users
  - Unauthorized attempts to use RACF commands
  - All RACF commands issued by users who have SPECIAL authority
  - Changes to any RACF profiles

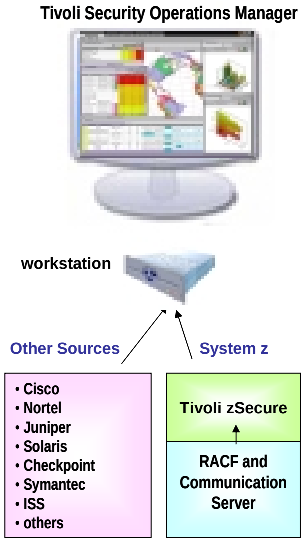
Extend z/OS and RACF Capabilities with Tivoli zSecure Tools

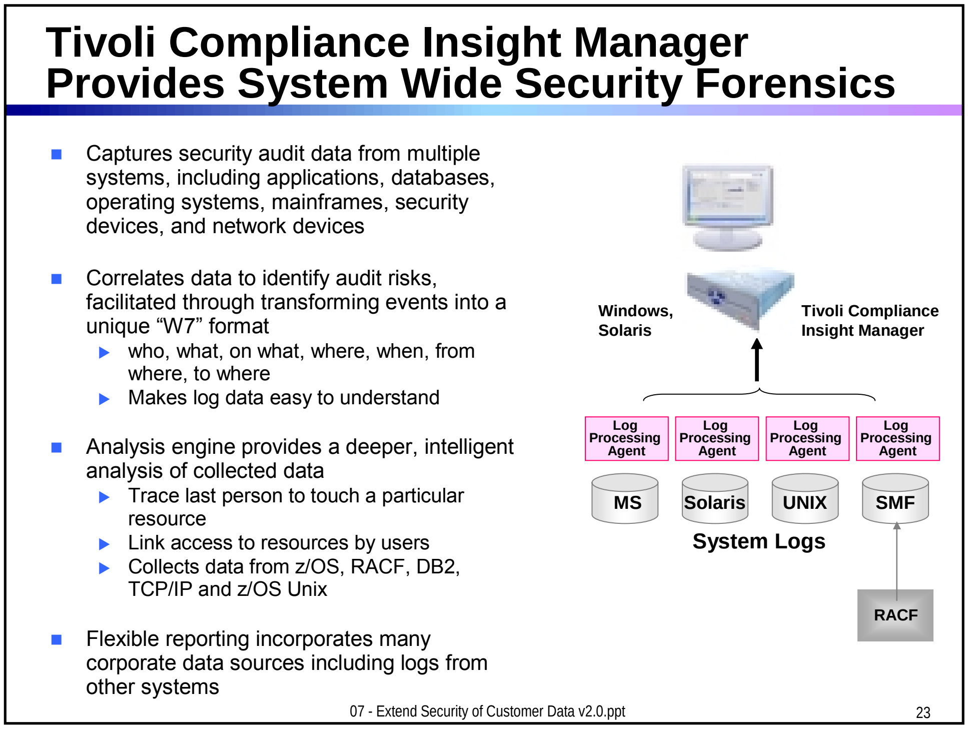
- Tivoli zSecure Alert
  - Provides real-time threat monitoring for z/OS and RACF
  - Can issue alerts when conditions occur
  - Can take action to stop security breaches
- Tivoli zSecure Audit
  - An audit and reporting tool for the mainframe
  - Built-in knowledge base identifies exposures
  - Provides real-time exception alerts
  - Can check integrity of sequential log data residing on tape or disk
- Tivoli zSecure Command Verifier
  - Prevent erroneous RACF commands from executing
  - Helps prevent errors
- Tivoli zSecure Admin
  - An enhanced administrative tool designed for the power user



Tivoli Security Operations Manager (TSOM)

- A dashboard for real time security alerts
- Improves effectiveness and visibility of security operations
- Analyzes system and network events to determine policy exceptions
  - Enables investigation and response to incidents
  - Streamlines incident tracking
  - Helps monitor and enforce policy
  - Advanced correlation to isolate root cause of security incidents
- Tivoli Security Operations Manager can consolidate mainframe alerts from over 200 event & log sources





Tivoli Compliance Insight Manager Provides System Wide Security Forensics

- Captures security audit data from multiple systems, including applications, databases, operating systems, mainframes, security devices, and network devices
- Correlates data to identify audit risks, facilitated through transforming events into a unique "W7" format
  - who, what, on what, where, when, from where, to where
  - Makes log data easy to understand
- Analysis engine provides a deeper, intelligent analysis of collected data
  - Trace last person to touch a particular resource
  - Link access to resources by users
  - Collects data from z/OS, RACF, DB2, TCP/IP and z/OS Unix
- Flexible reporting incorporates many corporate data sources including logs from other systems

Windows, Solaris

Tivoli Compliance Insight Manager

Log Processing Agent

Log Processing Agent

Log Processing Agent

Log Processing Agent

MS

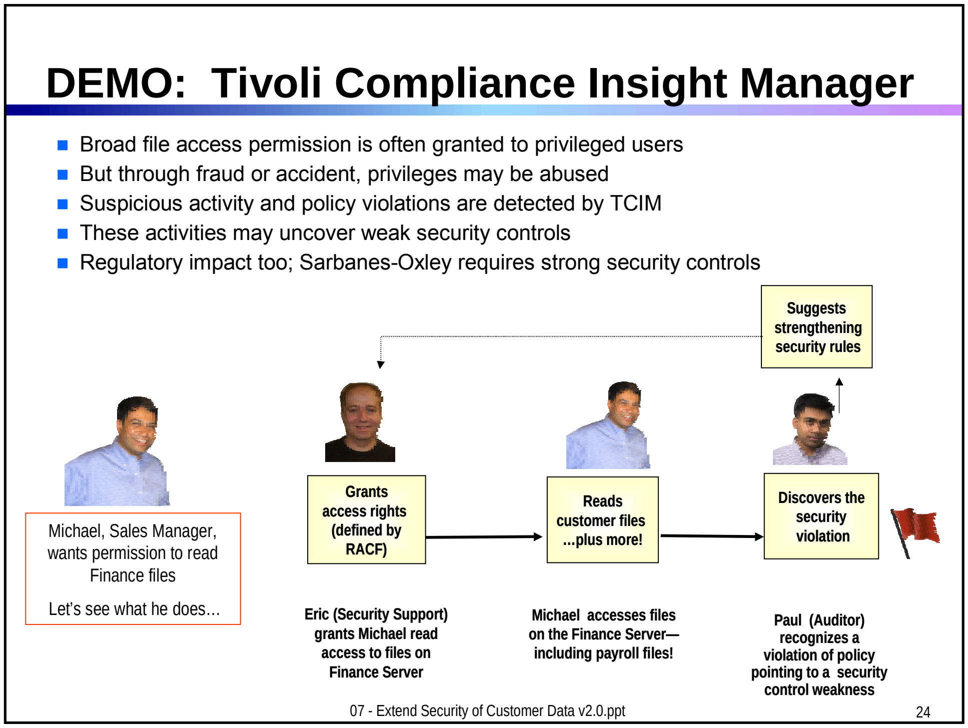
Solaris

UNIX

SMF

System Logs

RACF



DEMO: Tivoli Compliance Insight Manager

- Broad file access permission is often granted to privileged users
- But through fraud or accident, privileges may be abused
- Suspicious activity and policy violations are detected by TCIM
- These activities may uncover weak security controls
- Regulatory impact too; Sarbanes-Oxley requires strong security controls

Suggests strengthening security rules

Michael, Sales Manager, wants permission to read Finance files

Let's see what he does…

Grants access rights (defined by RACF)

Reads customer files …plus more!

Discovers the security violation

Eric (Security Support) grants Michael read access to files on Finance Server

Michael accesses files on the Finance Server—including payroll files!

Paul (Auditor) recognizes a violation of policy pointing to a security control weakness

Mainframe Extension Solution – Data Security Make the Most of What You Already Have!

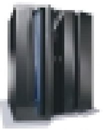
System z	**System z trusted base**	**Workload isolation and storage protection, common criteria evaluation**
	z/OS	Avoid need for extra virus control mechanisms or firewalls with System z architecture
	SMF, RACF	Built in logging with SMF records in a consistent format, turn on logging, use RACF to log events
Data Security	**RACF**	MLS capabilities of RACF, DB2 provide granular security to support different classification schemes
	CPACF	Entitled Clear key cryptography on every processor and IFL
	EKM	Provides the ability to issue, maintain and retrieve cryptographic keys
Communications	**z/OS Communications Server**	Provides intrusion defense , policy management as well as secured communications
	AT –TLS	Communications Server of System z provides easily accessible encrypted communications for applications

Further extend security

Encryption	**TS 1120 tape drive and C06 CU**	Secured tape drive with encryption capabilities built in
	2 Crypto Express2 Cards	Buy crypto cards for acceleration and co-processing
	zIIPs (Comm Server + zIIP)	Leverage zIIPs for IPSec
Compliance And Testing	**zSecure**	Simplifies administration and provides auditing analysis tools
	TSOM	Tivoli Security Operations Manager provides advanced network and systems security event management
	TCIM	Tivoli Compliance Insight Manager provides auditing and compliance reporting
	Optim	Optim provides testing while protecting data confidentiality

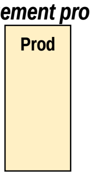
Mainframe Extension Solution – Deploy New Security Capabilities

Existing Mainframe



Existing processors:
2 general purpose
4000 MIPS, 1 zIIP, Tape CU
DB2 workload
z/OS, RACF,
Communications Server

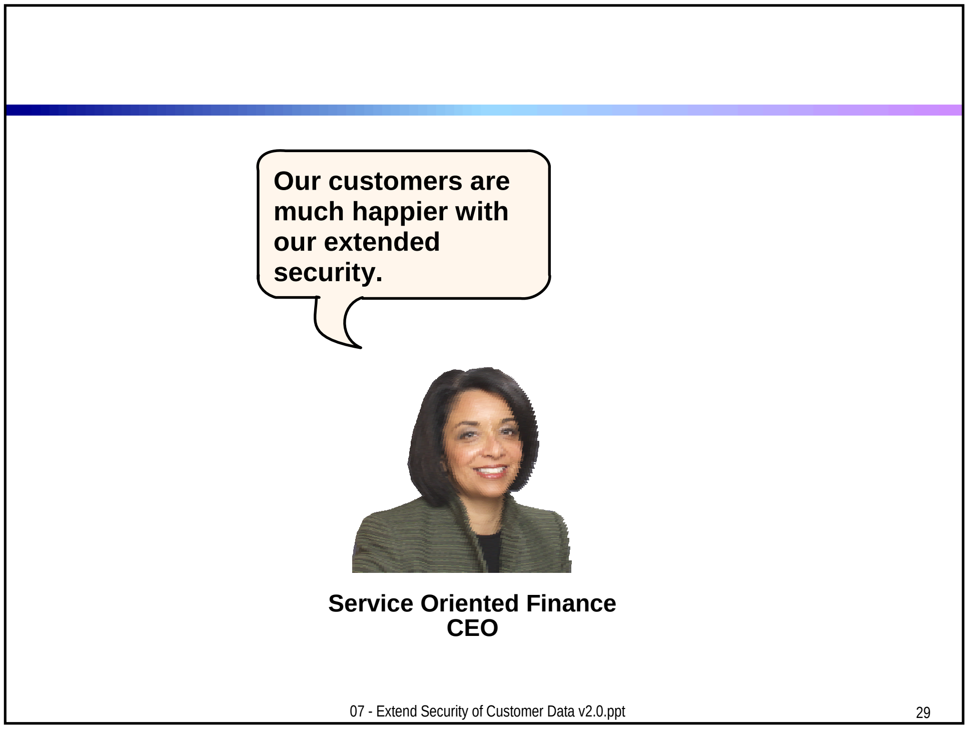
Add mainframe compliance & management products



Add hardware
- 1 zIIP for IPSec
- 2 TS1120 tape drives
- 2 Crypto Express2 cards
- 2 Intel servers

Add software
- zSecure
- TSOM
- TCIM
- Optim

3 year cost of acquisition $4M



Our customers are much happier with our extended security.

Service Oriented Finance
CEO