Extending Your Mainframe For More Business Value

Extend Data Security On The Mainframe

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**
  - Detect and prevent intrusions
- **Establish and monitor security compliance policies**
  - Detect breaches of policy

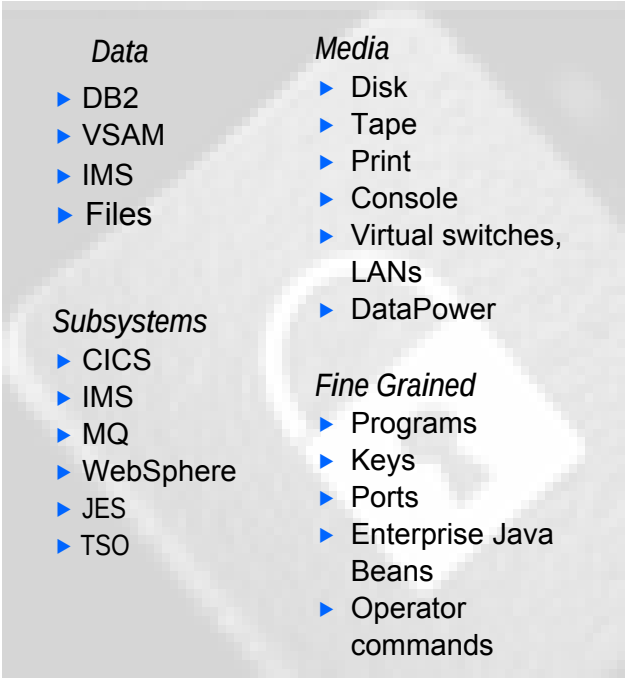
A Secure Foundation Is A Prerequisite To Address Security Issues

- **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
- **System z has the highest commercial common criteria ratings**
  - PR/SM rated at EAL 5
- **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
  - System z10 delivers stronger encryption using Advanced Encryption Standard (AES) 192 and 256, and SHA-384 and SHA-512

System z Provides 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
- **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

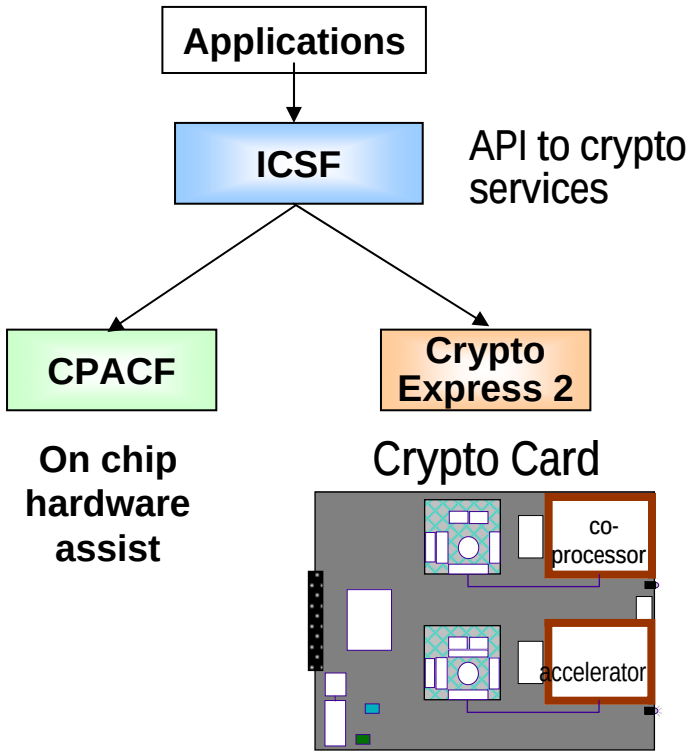
Resources Protected by RACF



Manage all your resources consistently as you build out new applications

*** Resource Access Control Facility**

Built In Encryption On System z Protects Data Privacy

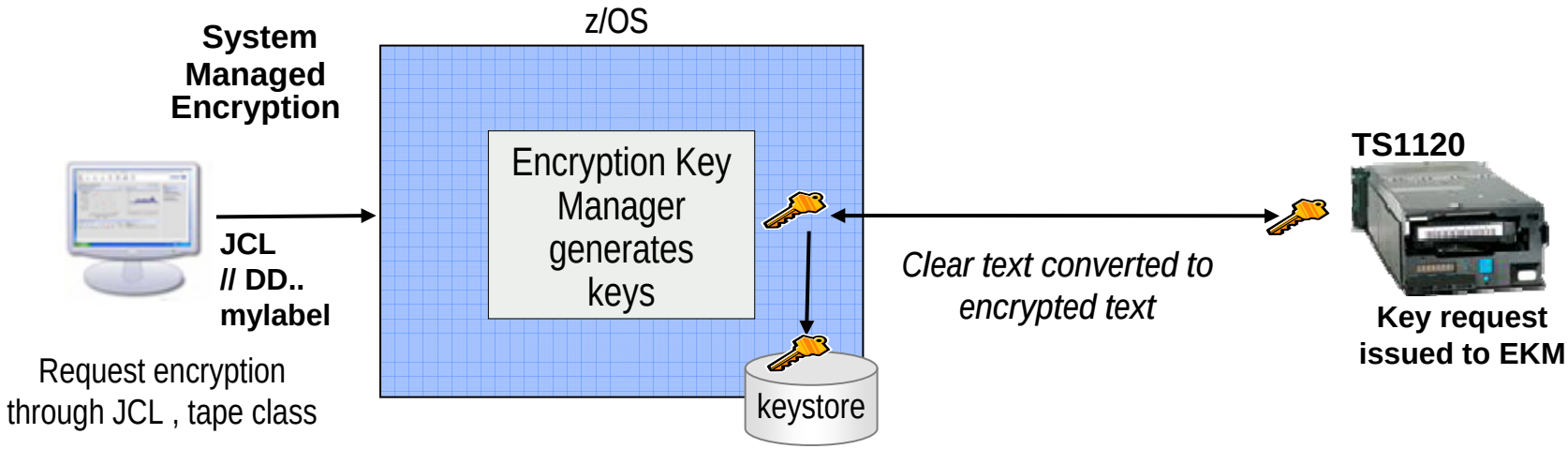


- **Central Processor Assist for Cryptographic Function (CPACF)**
  - A CP Assist for Cryptographic Function (CPACF) is on CPU chip
  - Provides clear key encryption
- **Crypto Express2 Card**
  - High performance cryptography for SSL
    - 6,000 handshakes per second
  - Secure key cryptography
  - Dynamically configurable
    - Co-processor or Accelerator
  - FIPS 140-2 Level 4 compliant
  - Clears out memory if tampered with
- **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!



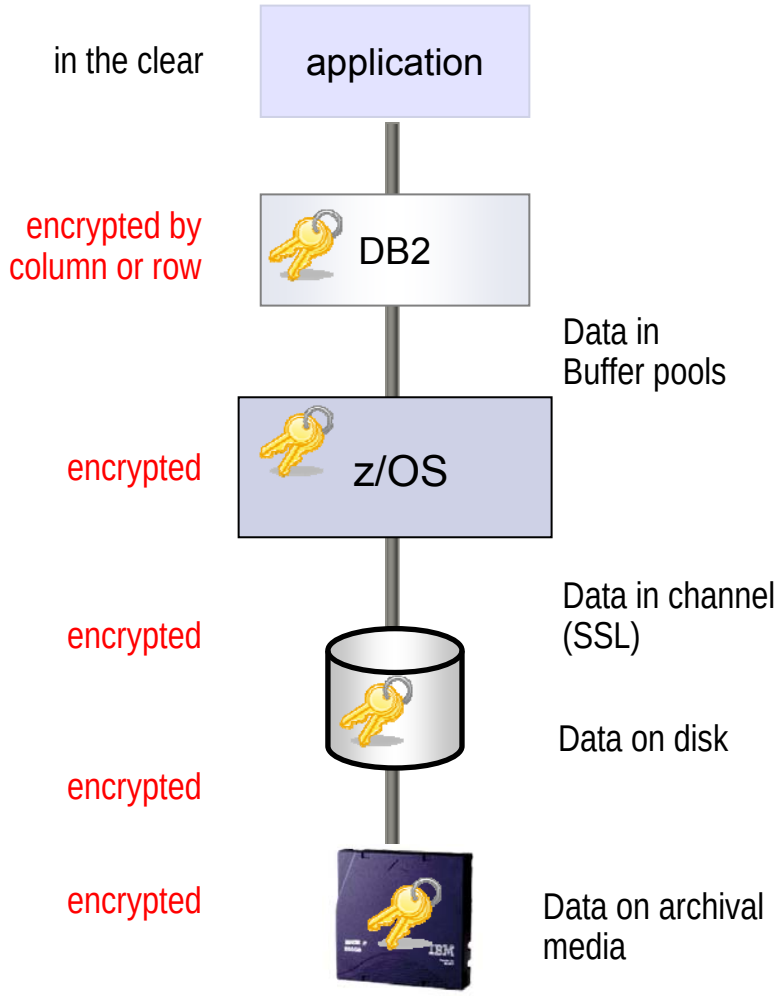
System z Encryption Key Management

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
  - Can retrieve required keys from protected key stores
- **Options to store the keys**:
  - RACF-protected key stores
  - Uses tamper-resistant crypto cards to store “secure keys”
  - Other protected data sets, files
- **New Tivoli Key Lifecycle Manager extends usability and reach**

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
- Prevents reclassification of information

DB2 Multi-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

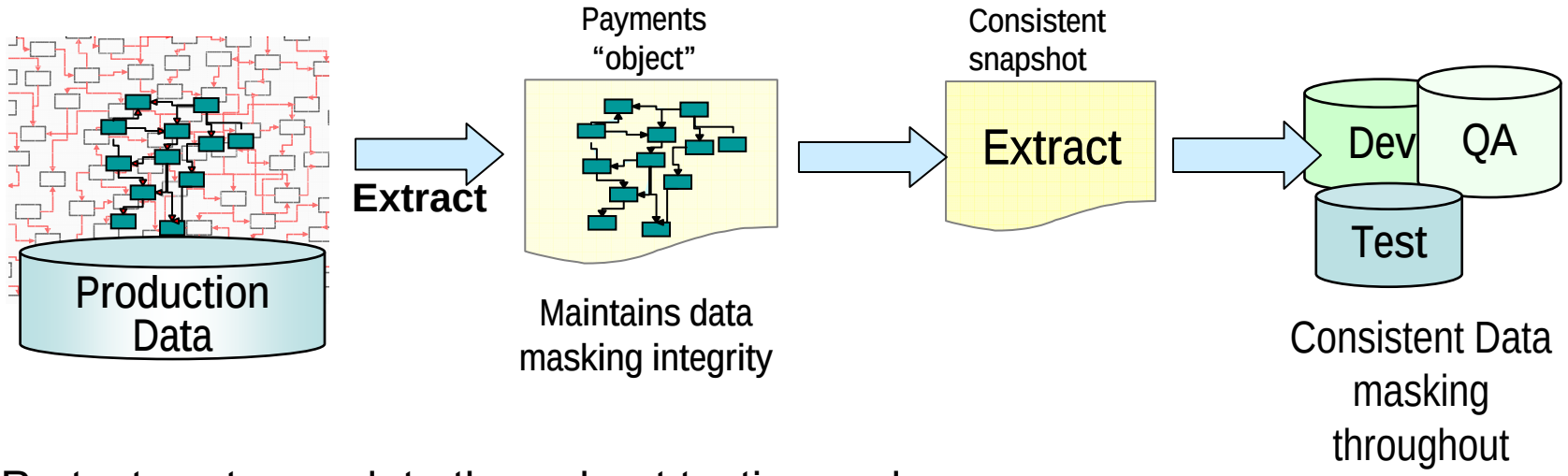
Underwriter

Claims Analyst

National Broker

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%

Don’t Forget To Protect Customer Data During Testing Of New Releases



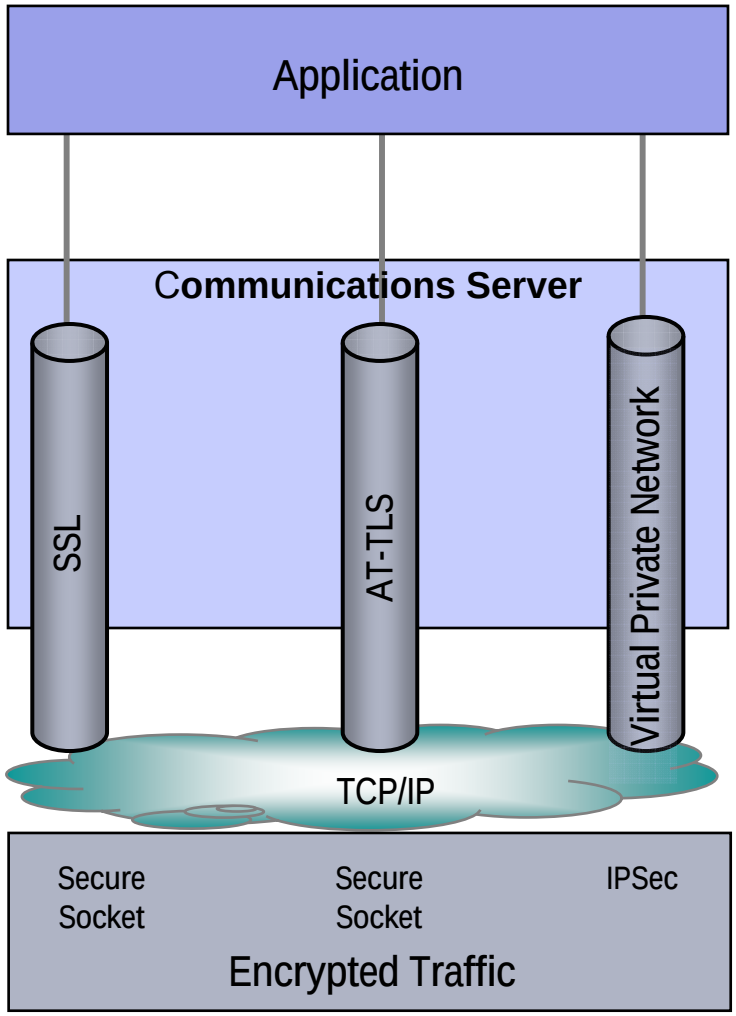
- Protect customer data throughout testing cycle with Optim
- Customer data can be compromised during testing cycles, especially during audits
- Mask or replace customer data with fictional data in a consistent manner preserving the integrity of data relationships
- Extract a snapshot for testing purposes
- Helps ensure privacy of data shipped to outsourcers

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
  - Defensive IP filtering (built-in firewall)
- 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
- SSL and IPSec processed by crypto processor if available
  - IPSec can be offloaded to zIIP

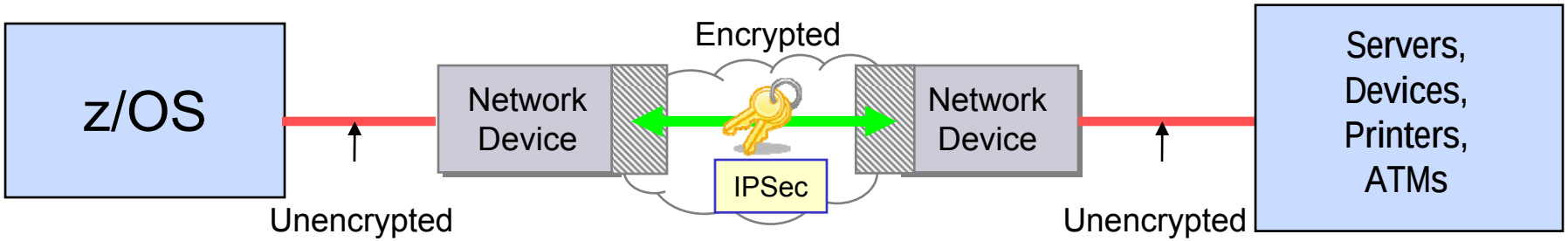


*AT-TLS= application transparent transport level security

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.

System z – End-to-end encryption

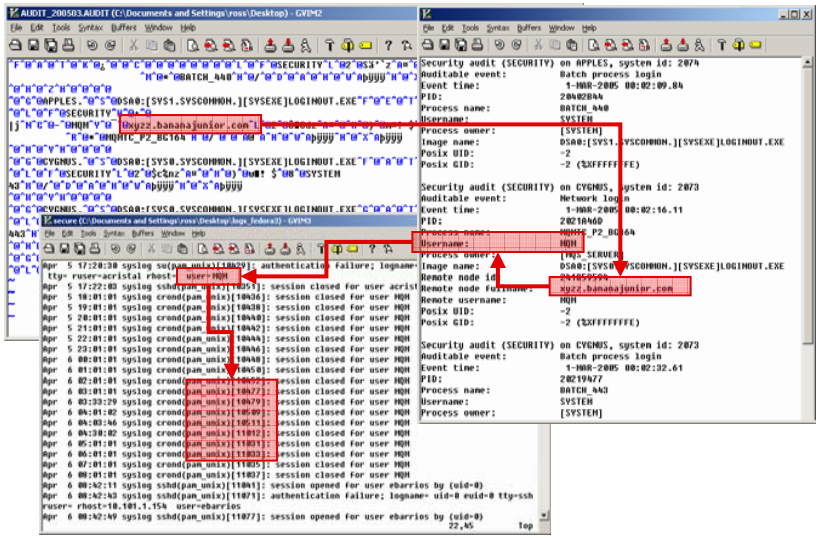


Encryption with routers can leave gaps

RACF Security Event Logging

- RACF helps audit access attempts
  - Started during IPL to prevent vulnerabilities from being introduced
  - Audit control functions specify information RACF should log
  - SMF log datasets themselves are protected

- RACF logs many events:
  - Accesses to data sets, resources
  - Accesses to a specified class of resources at a specified access level
  - RACF-related activities of specific users
  - Unauthorized attempts to use RACF commands
  - RACF commands issued by users with SPECIAL authority
  - Changes to RACF profiles

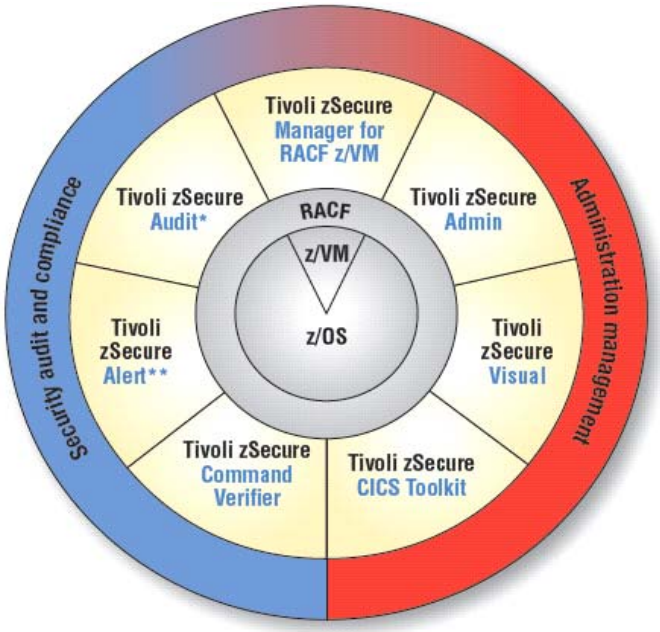


With other systems, customers have to manually make sense out of all these different log formats

Tivoli zSecure Suite Extends System z Security Management

- Tivoli zSecure Alert
  - Can issue alerts when conditions occur, taking action to stop breaches
  - Provides real-time threat monitoring for z/OS and RACF
  - RACF offline option simulates impact of RACF changes
- Tivoli zSecure Audit
  - Provides real-time exception alerts
  - An audit and reporting tool for the mainframe
  - Built-in knowledge base identifies exposures
- Tivoli zSecure Command Verifier
  - Prevent execution of erroneous RACF commands

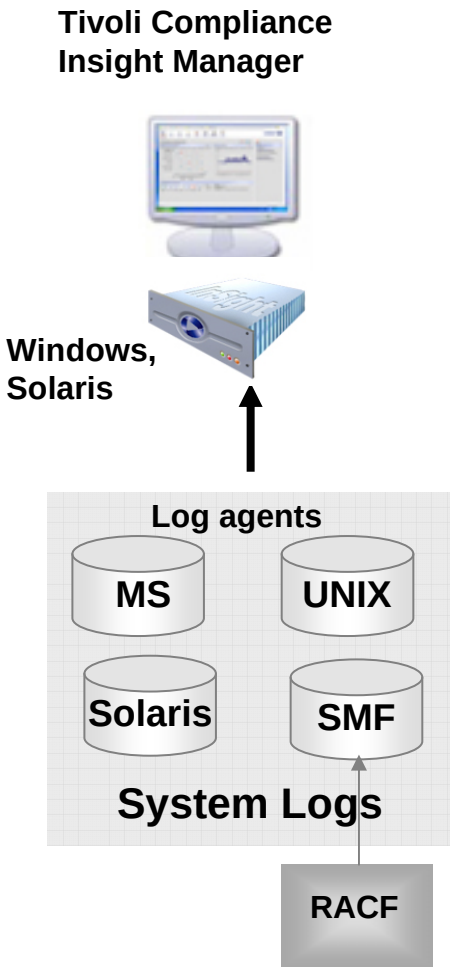
Tivoli zSecure Suite



*Also available for ACF2™ and Top Secret®
**Also available for ACF2

Tivoli Compliance Insight Manager Security Management In Support Of Regulations

- Sarbanes-Oxley Section 404 specifies the need to implement controls designed to prevent or detect fraud
  - I.e. separation of incompatible business duties or responsibilities
- TCIM helps detect regulatory and policy violations
- Captures log data from multiple sources
- Correlates data to identify and investigate audit risks
  - Uses unique “W7” format to make log data understandable
  - Helps determine who acted upon what resource



DEMO: Tivoli Compliance Insight Manager

- Sarbanes-Oxley requires implementation of strong security controls
- However, broad privileges may be granted to authorized users
- Through either fraud or accident, privileges *may* be abused
- This can lead to a violation of *segregation of duties*
- Suspicious activity detected by TCIM helps identify weak controls, which then can be strengthened to prevent further abuse

Michael, Sales Manager, wants permission to read Finance files

Let's see what he does…

Grants access rights (defined by RACF)

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

Reads customer files …plus more!

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

Discovers the security violation

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

Suggests strengthening security rules

Mainframe Extension Solution – Data Security
Make The Most Of What You Already Have!

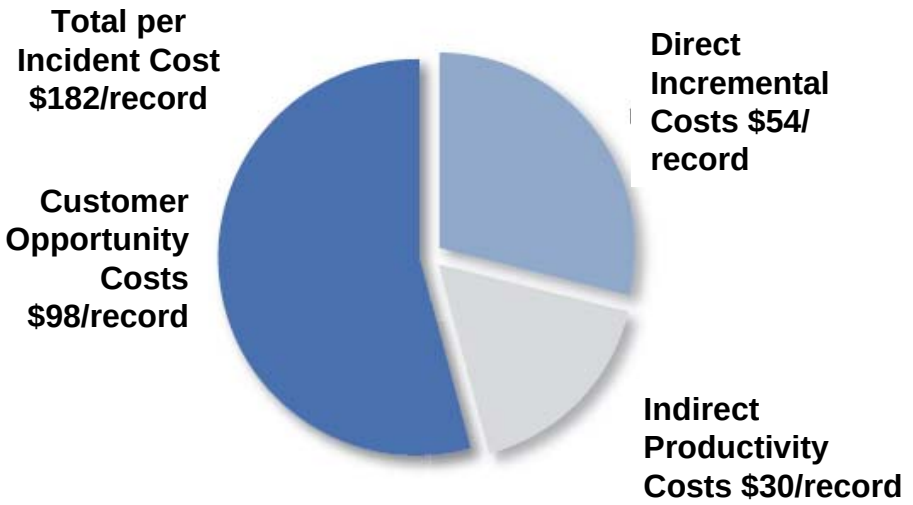
System z	System z trusted base	Workload isolation and storage protection, common criteria evaluation
	z/OS	Avoid need for extra virus control mechanisms or firewalls with System z architecture
	SMF, RACF	Built in logging with SMF records in a consistent format, turn on logging, use RACF to log events
Data Security	RACF	MLS capabilities of RACF, DB2 provide granular security to support different classification schemes
	CPACF	Entitled clear key cryptography
	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
	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

The Cost Of A Data Security Breach

- **Total per-incident costs** including average direct, indirect, and opportunity costs:
  - $182 per record, or $4.8M per company
- Range of surveyed breach costs:
  - $226K to $22M per incident
- Each incident resulted in an average 2% loss of existing customers
  - Worst case was 7%



Ponemon Study: 2006 Survey Cost of a Data Breach

Case Study: Mainframe Extension Solution – Deploy New Security Capabilities

Existing Mainframe

Existing z10:
6 GP 4,000 MIPS
1 zIIP
Tape CU
DB2 workload
z/OS, RACF
Communications Server

Add mainframe compliance & management products

Prod

Incremental:
1 zIIP for IPSec
2 TS1120 tape drives
2 Crypto Express2 cards
2 Intel servers
zSecure
TSOM/ TCIM bundle
Optim

3 year cost of acquisition $3.83M

According to the Ponemon Study, *the average incident costs are $4.8M*