IBM's System z Forum

Is Your Mainframe Data as Secure as you Thought?

John McKinnon
Data Governance Technical Lead, AP

Agenda

- Introduction
- Masking Data with Optim Test Data Management
- Auditing Data on System Z
- Encrypting Data on System Z

Introduction

What happens when you're NOT in control of your business data…

Health Care - *Dozens of women were told wrongly that their smear test had revealed a separate infection after a hospital error, an independent inquiry has found….*

…Confusion arose because the hospital decided to use a code number to signify "no infections", not realizing that it was already in use at the health authority where it meant "multiple infections".

Retail - *Hackers have stolen 4.2 million credit and debit card details from a US supermarket chain by swiping the data during payment authorization transmissions in stores.*

Banking - *A major US Bank has lost computer data tapes containing personal information on up to 1.2 million federal employees, including some members of the U.S. Senate.*

The lost data includes Social Security numbers and account information that could make customers of a federal government charge card program vulnerable to identity theft….”

Banking - *Rogue trader accused of the world's biggest banking fraud was on the run last night after fake accounts with losses of £3.7 billion were uncovered. The trader used his knowledge of the bank's control procedures to hack into its computers and erase all traces of his alleged fraud.*

….Mr Leeson said: "Rogue trading is probably a daily occurrence within the financial markets. What shocked me was the size. I never believed it would get to this degree of loss."

Public Sector - *Two computer discs holding the personal details of all families in the UK with a child under 16 have gone missing.*

The Child Benefit data on them includes name, address, date of birth, National Insurance number and, where relevant, bank details of 25 million people….”

“WASHINGTON – The FINRA announced today that it has censured and fined a Financial Services company $370,000, for making hundreds of late disclosures to FINRA's Central Registration Depository (CRD) of information about its brokers, including customer complaints, regulatory actions and criminal disclosures. "Investors, regulators and others rely heavily on the accuracy and completeness of the information in the CRD public reporting system - and, in turn, the integrity of that system depends on timely and accurate reporting by firms,"

…. Resulting in a broad range of potentially life threatening consequences

Health Care - Dozens of women were told wrongly that their smear test had revealed a sexually transmitted infection after a hospital error, an independent inquiry has found.…

Incorrect classification..

Life threatening consequences

…Confusion arose because the hospital's computer system used the code number to signify "no infections", not realizing that it was already in use at the health authority where it meant "multiple infections".

Ineffective Security..

Brand damage

Financial loss

…Hackers have stolen 4.2 million credit and debit card details from a US supermarket chain by planting software on payment authorization transmissions in stores.

Banking - A major US Bank has lost computer data tapes containing personal information on up to 1.2 million current and former employees, including some members of the U.S. Senate.

Physical Data Loss..

Identity Theft

The lost data includes Social Security numbers and account information that could make customers of a federal government charge card program vulnerable to identity theft.…"

Banking - Rogue trader accused of the world's biggest banking fraud was on the run last night after fake accounts with losses of £3.7 billion were uncovered. The trader used his knowledge of the bank's control procedures to hack into its computers and erase all traces of his alleged fraud.

….Mervyn King said: "Rogue trading is probably a daily occurrence within the financial markets. What shocked me was the size. I never believed it would get to this degree of loss."

Poor Internal Controls..

Bankruptcy,

Financial ruin, penalties

Public Sector - Two computer discs holding the personal details of all families in the UK with a child under 16 are lost in the post.

The child benefit data on them includes name, address, date of birth, National Insurance number and, where relevant, bank details of 25 million people…"

Physical Data Loss..

Fraud on a massive scale

"WASHINGTON – The FINRA announced today that it has censured and fined a Financial Services company $370,000, for making hundreds of late disclosures to FINRA's Central Registration Depository (CRD) of information about registered representatives, including customer complaints, regulatory actions and criminal matters. Investors rely heavily on the accuracy and completeness of the information in the CRD public reporting system - and, in turn, the integrity of that system depends on timely and accurate reporting by firms."

Late Disclosures..

Heavy Fines

Legal implications and resignations

The Integrated Data Management Solution
5 essentials for protection and privacy

Discover Location of Sensitive Data

Automating the detection of sensitive data and enterprise data relationships

Strengths:

- ✓ *Discover hidden data relationships to define business groupings of data*
- ✓ *Automate detection of sensitive data*
- ✓ *Reverse engineer transformation logic and prototype data consolidation rules*

Mask data in non-production environments

Protect sensitive structured data in non-production environments (for dev, testing, offshore dev)

Strengths:

- ✓ *Best practice for protecting sensitive data and supporting the testing process*
- ✓ *Mask information in 1 or many places using realistic values*
- ✓ *Reduce impact of internal and external data breaches*

Monitor database activity & assess vulnerabilities

Provide essential safeguards to protect high value databases across heterogeneous environments

Strengths:

- ✓ *Continuous, real-time database access and activity monitoring*
- ✓ *Policy-based controls to detect unauthorized or suspicious activity*
- ✓ *Vulnerability assessment, change auditing & blocking*

Encrypt files in database environments

Protect database files to control the "who, what, when, where, and how" data can be accessed

Strengths:

- ✓ *Encrypt files with minimal application impact*
- ✓ *Separation of duties for role efficiency – DBA vs IT Security*
- ✓ *Unified policy and key management for central administration*

Redact unstructured data in documents

Protect stand-alone or embedded unstructured sensitive data in forms and documents

Strengths:

- ✓ *Support redaction of textual, graphical, and form based data*
- ✓ *Increase efficiency via automation and reduce cost of manual redaction*
- ✓ *Control the data viewed by each user with policy rules*

Satisfy compliance and regulatory mandates

Defense in Depth to protect your information

- **Optim Data Privacy**
  - Masking to protect sensitive data
- **Optim Data Growth Solution**
  - Data Retention and archiving
- **Guardium for Z Auditing**
  - Data Audit and monitoring
- **Guardium Data Encryption for IMS and DB2 databases**
  - Single tool for data encryption for IMS and DB2
- **Tivoli SIEM** (Security Information Event Management)
  - Compliance enterprise reporting
- **Infosphere Data Architect**
  - Capture Governance metadata

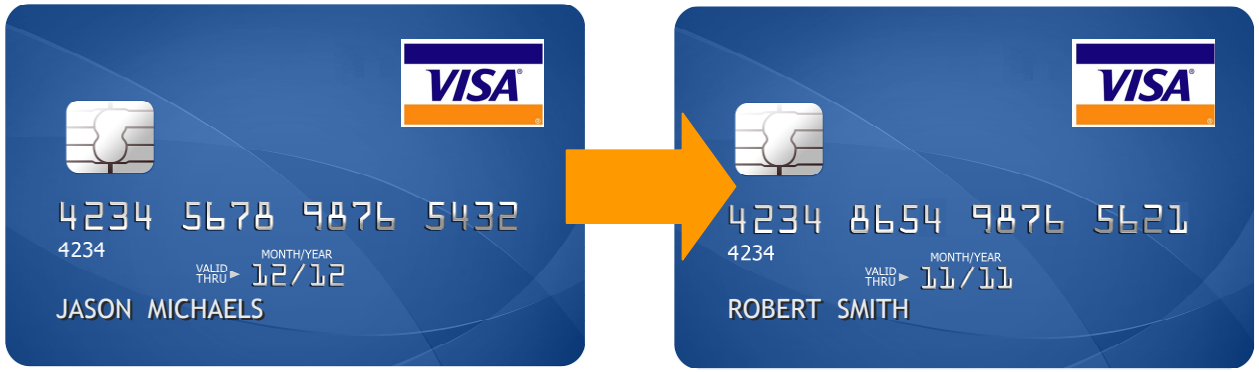
Attacks have moved beyond external hackers to internal breaches

➢ ***Protect the data at the source***

Masking Data with Optim Data Privacy

IBM InfoSphere Optim Data Masking Solution

De-identify sensitive information with realistic *but fictional* data for testing & development purposes



Personal identifiable information is masked with realistic but fictional data for testing & development purposes.

Requirements

- Protect confidential data used in test, training & development systems
- Implement proven data masking techniques
- Support compliance with privacy regulations
- Solution supports custom & packaged ERP applications

Benefits

- Protect sensitive information from misuse and fraud
- Prevent data breaches and associated fines
- Achieve better data governance

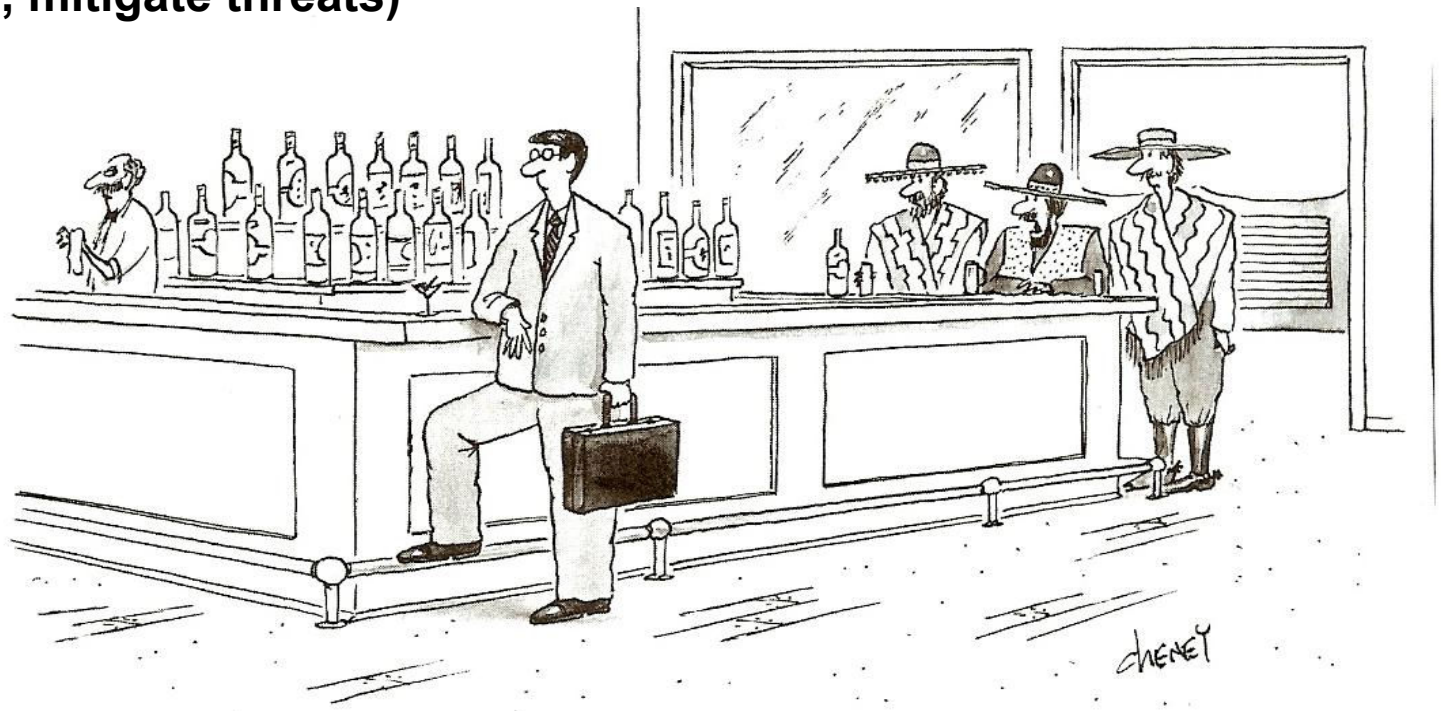
Optim Data Privacy z/OS Solutions

- **IBM Optim Data Privacy Solution for z/OS v2.1**
  - The core data privacy solutions for custom DB2 z/OS applications
- **IBM Optim Data Privacy Solution PCI Module for z/OS v2.1**
  - A subset of the *IBM Optim Data Privacy Solutions*
  - Supports Payment Card Industry Data Security Standard 6 and 7
  - Contains all Replacement Data
  - Only a subset of the Identify Model data privacy policies are included
    - Person, Credit Card, Address, Email, National ID and Names
  - The Date and Scramble model data privacy policies **are not** included
- **IBM Optim Data Privacy Solution for z/OS for SAP v1.2.2**
  - Contains all the core functionality of the Data Privacy Solution
  - Contains pre-packaged models and services for SAP R/3 4.6C & 4.7
  - Has not been migrated to v2.1
  - Does not use the new v2.1 architecture
  - Still uses the v1.2 architecture and user interfaces

Auditing Data Access on z/OS

Why Do Organizations Buy Database Activity Monitoring?

1. **Someone told them they have to (regulations – auditors)**
2. **They're tired of the cost & effort of doing it manually (no time, spending lots of money, other DBA's priorities)**
3. **They know it's the right thing to do, long-term (optimization, secure controls, mitigate threats)**



"It's him – the one they call 'El Auditor.'"

Harvard Business Review

ation

Customer Challenges: Auditing on z/OS

- Regulatory pressures to demonstrate adequate controls
  - Especially around privileged users (DBAs, SYSADMs, …)
- Most z/OS environments have minimal auditing
  - Requires significant manual effort by DBAs
- RACF sometimes perceived as sufficient security control, but RACF does not:
  - Prevent unauthorized update if the user has authority to the data
  - Prevent access to sensitive data that is not within scope of their job
  - Capture a granular audit trail of what the user did while accessing DB2
- Does not support Separation of Duties (SoD) + represents security risk and exposure
  - DB2 trace processes managed by DBAs that are being monitored

Is this Really a problem on Z?

- **We've enjoyed 45+ years of no known external hacking on mainframes!**
- **System Z is the most secure platform, right?**
- **RACF keeps the baddies out**
- **Our DBAs control all the auditing**

Questions we are often asked…

What we hear:

- **"We control who is connected to the DB2 SYSADM group and we know what those people are authorized to do"**
- **"We have RACF!"**

- **Yes, but…**
  - **RACF does two things:**
    - **Prevents people from accessing a resource that is not essential or appropriate for their jobs**
    - **Allows people access to the necessary data to do their jobs**
  - **But RACF does NOT:**
    - **Prevent a malicious update if the user has authority to the data.**
    - **Prevent an authorized user from accessing sensitive data that is *NOT* within the scope of their job.E.g. a bank teller looks up the CEOs bank balance or personal customer information**
    - **Provide meaningful information about access to protected DB2 resources (authorized or not)**
  - **Auditors will want proof that your solution is (and remains) unbiased throughout its life span, and that it provides segregation of duties**
  - **It only takes one employee or contractor to accidently or maliciously divulge the data**

You need both robust security and fine-grained auditing in order to adequately protect the database environment .

Questions we are often asked…

Quis custodiet ipsos custodes?

Who watches the watchers?

Guardium Data Security Portfolio for System z

Discover Location of Sensitive Data

Automating the detection of sensitive data

Strengths:

- ✓*Automate detection of sensitive data*
- ✓*Integrate objects within Security Policies*
- ✓*Integrates with InfoSphere Discovery to build business object and data relationships*

InfoSphere Guardium

Vulnerability Assessment

Assess Risk and provide remediation recommendations

Strengths:

- ✓*Configuration and security best practices*
- ✓*Patch management verification*
- ✓*Custom SQL Assessment tests*
- ✓*Supports System z and distributed*

InfoSphere Guardium VA

Monitor database activity

Provide essential safeguards

Strengths:

- ✓ *Continuous, real-time database access and activity monitoring*
- ✓*Policy-based controls to detect unauthorized or suspicious activity*
- ✓*Workflow to satisfy compliance requirements*

InfoSphere Guardium DAM

Encrypt files in database environments

High performance data encryption

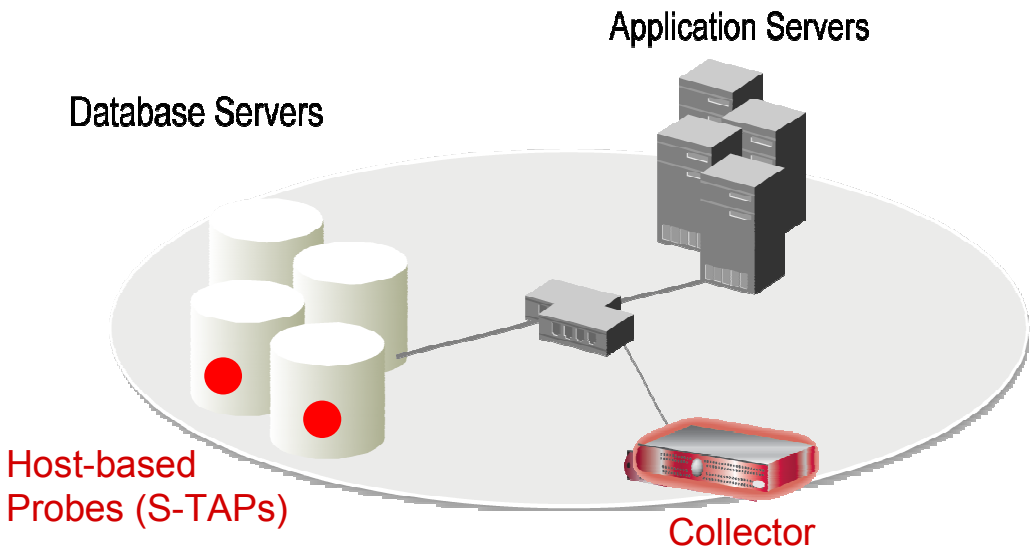
Strengths:

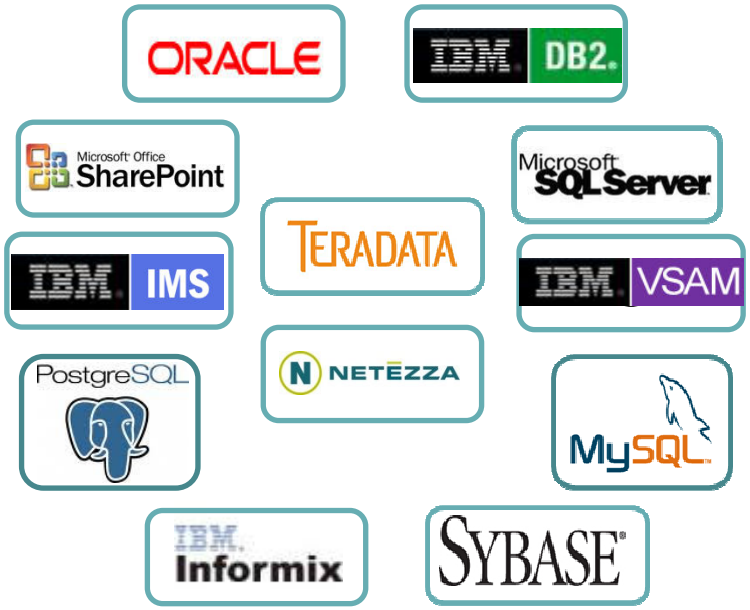
- ✓ *Encrypt files with minimal application impact*
- ✓*Separation of duties for role efficiency – DBA vs IT Security*
- ✓*Unified policy and key management for central administration*

Guardium Data Encryption for DB2 & IMS

Satisfy compliance and regulatory mandates

Real time database monitoring & protection

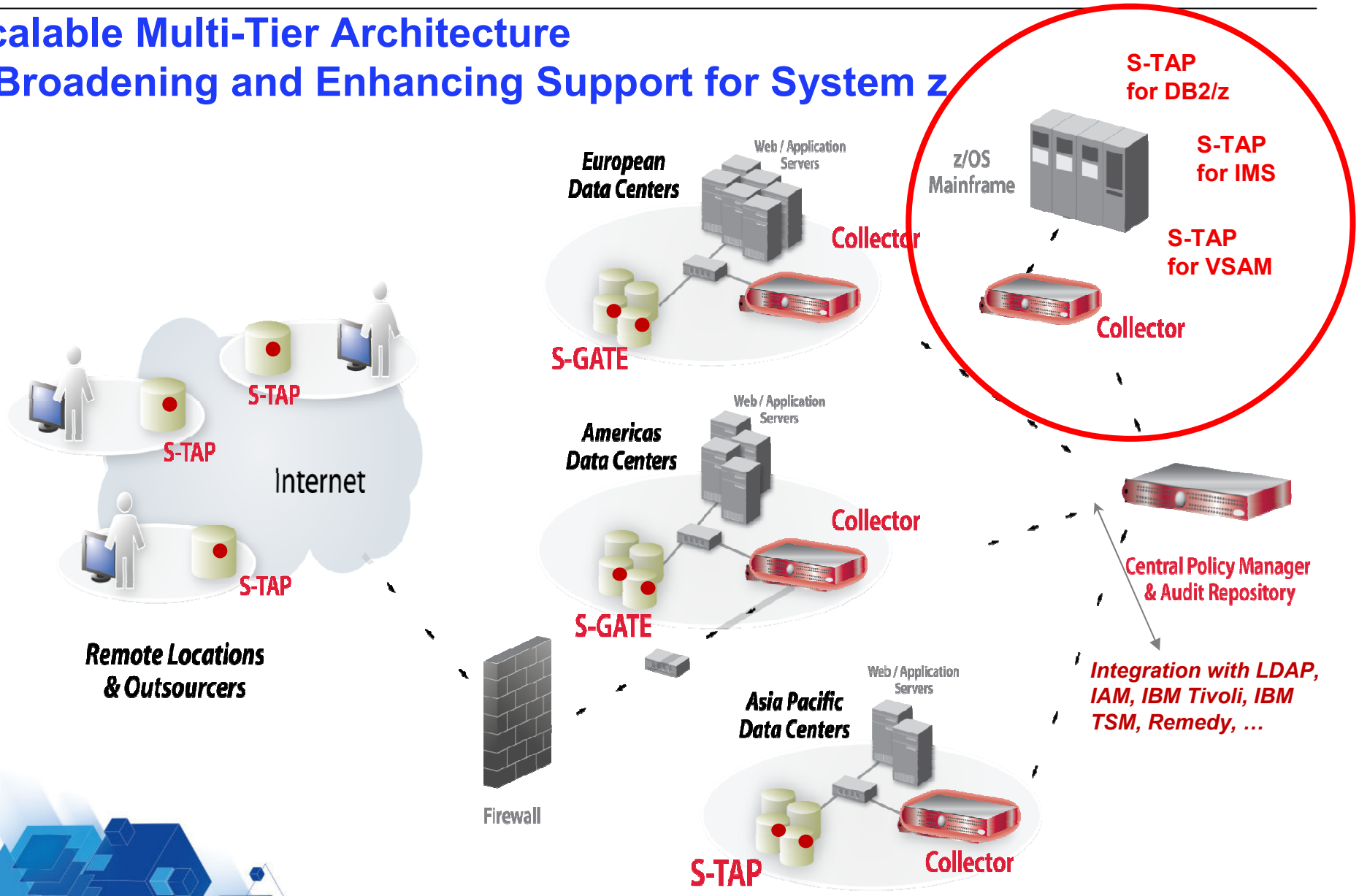




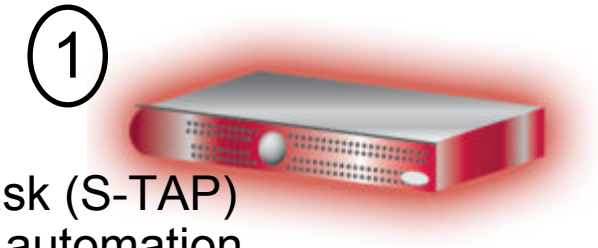
- Separation of Duties
- No DBMS or application changes
- Does not rely on DBMS-resident logs that can easily be erased by attackers, rogue insiders
- 100% visibility including local DBA access
- Minimal performance impact

- Cross-DBMS solution
- Granular, real-time policies & auditing
  - *Who, what, when, how*
- Automated compliance reporting, sign-offs and escalations (financial regulations, PCI DSS, data privacy regulations, etc.)

Scalable Multi-Tier Architecture
Broadening and Enhancing Support for System z



Guardium for z – (2) components

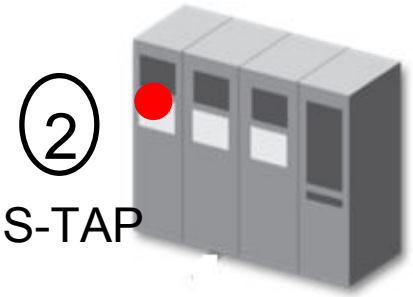


1. Guardium hardware or software appliances

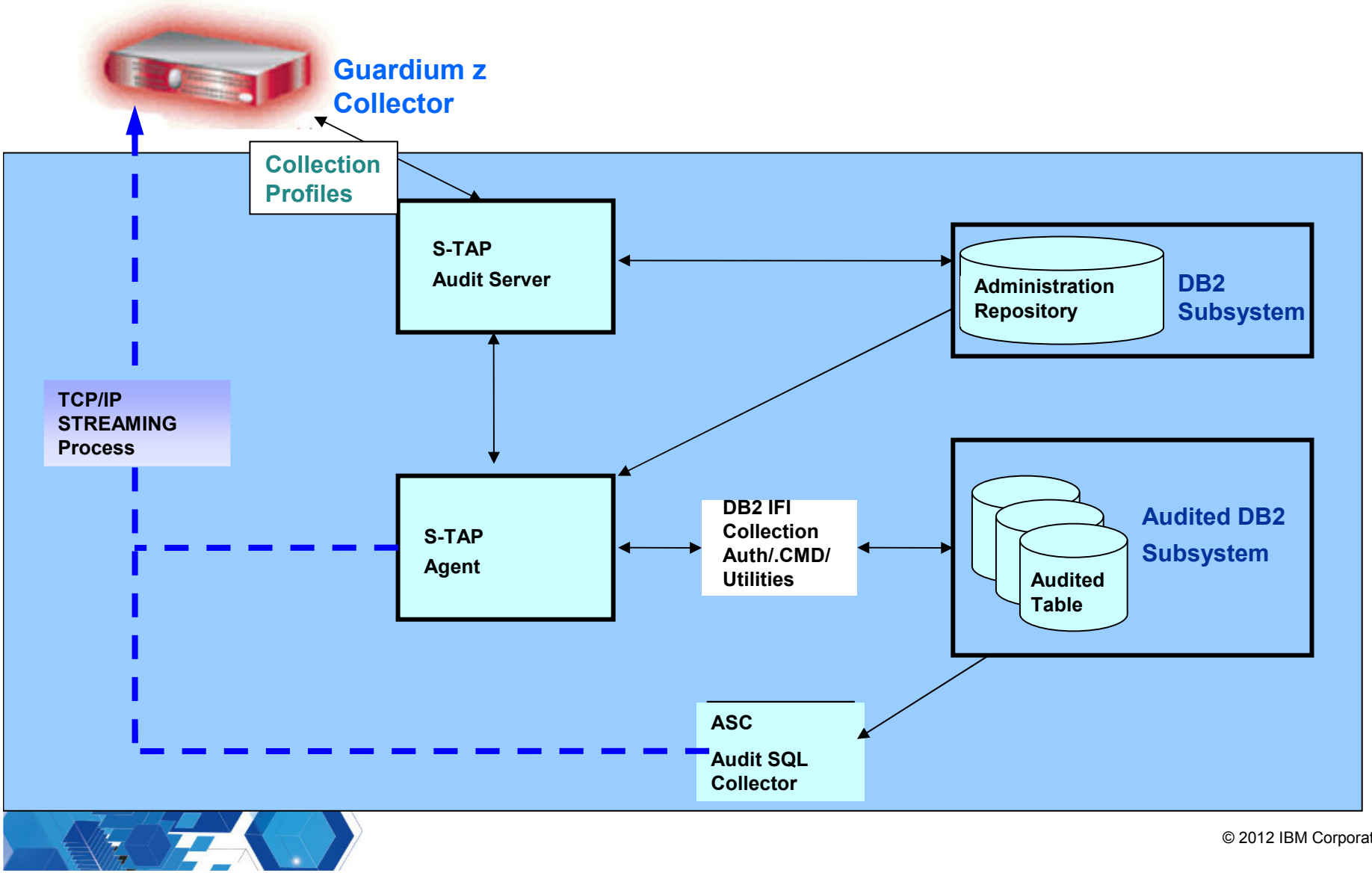
- Securely stores audit data collected by mainframe task (S-TAP)
- Provides analytics, reporting & compliance workflow automation
  - Offloads audit data processing from mainframe
- Integrated with Guardium enterprise architecture
  - Centralized, cross-platform audit repository for enterprise-wide analytics and compliance reporting across System z & distributed environments
    (Oracle, SQL Server, DB2, Informix, Sybase, MySQL, Teradata)

2. S-TAP for System z

- Mainframe task
- Collects and streams audit data to Collector appliance
- Leverages existing IBM DB2/z collection technology
- In the Guardium context, we order 5655-xxx



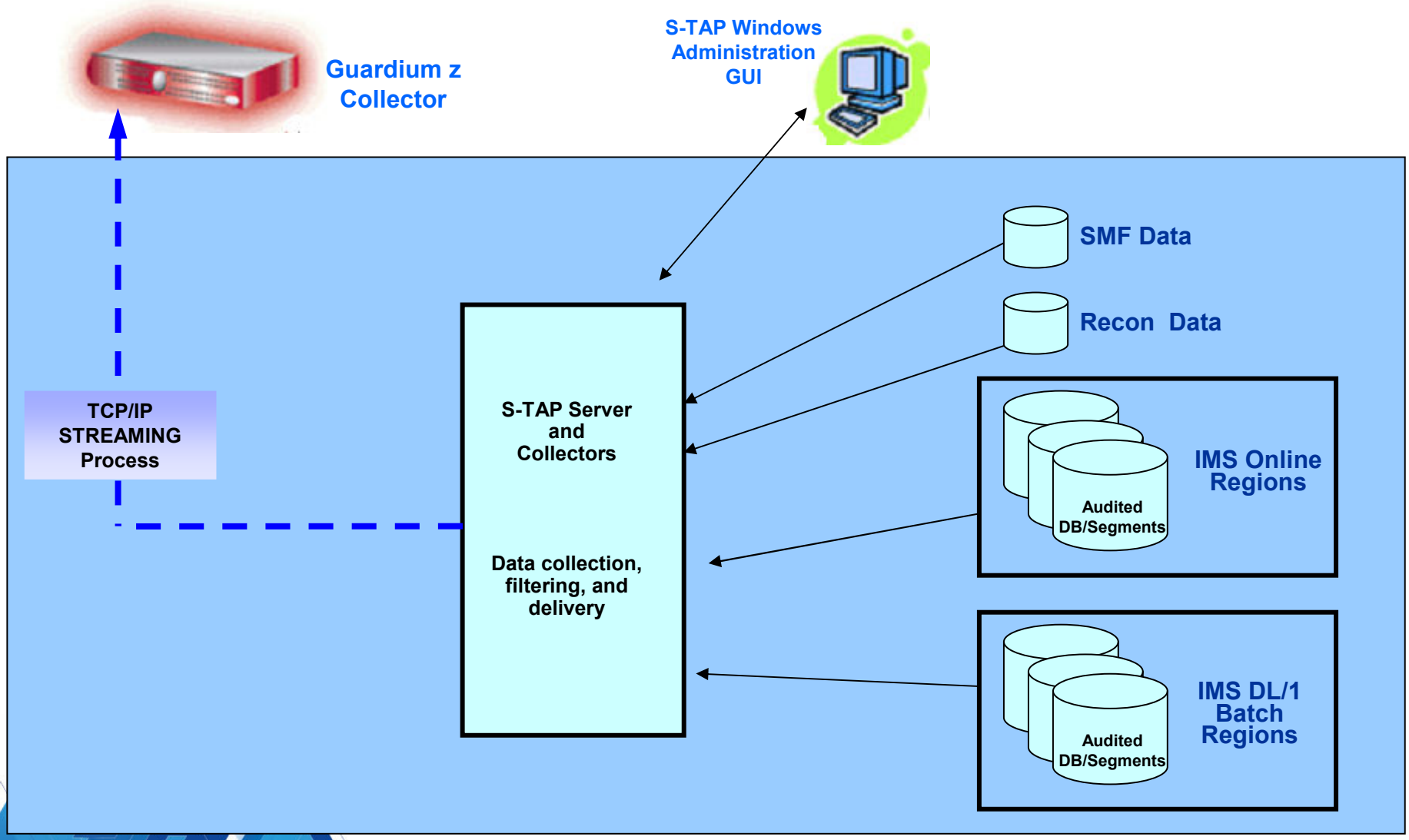
Guardium S-TAP for DB2 on z/OS Architecture



Guardium S-TAP for IMS on z/OS - New(ish) Product

- **Introducing new S-TAP for collecting IMS DB events**
- **What IMS events can we collect?**
  - Databases
    - READ accesses to databases
    - Changes, INSERT, UPDATE and DELETE calls
    - Same for IMS Batch jobs and IMS Online regions
  - Segments
    - Ability to audit and report READ, INSERT, UPDATE, and DELETE calls on specific database segments
  - Access to IMS related information outside of IMS control
- When a call is to be collected, the relevant information is gathered and streamed to the Guardium for z appliance

Guardium S-TAP for IMS on z/OS Architecture (1)



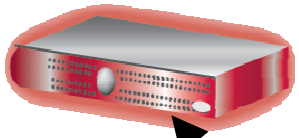
Guardium S-TAP for VSAM on z/OS - New(ish) Product

New S-TAP for collecting VSAM events

•Useful for monitoring datasets related to the DBMS and access bypassing the DBMS

- File types: ESDS, KSDS, RRDS, VRRDS, and LDS
- Events:
  - DATA SET OPEN
  - DATA SET OPEN for UPDATE
  - DATA SET DELETE
  - DATA SET RENAME
  - DATA SET CREATE
  - DATA SET ALTER
  - RACF ALTER
  - RACF CONTROL
  - RACF UPDATE
  - RACF READ

Guardium S-TAP for VSAM on z/OS Architecture



Guardium Appliance

Collection Policy

z/OS

TCP/IP

S-TAP STC

FILTER EVENT DATA

AGENT

CONTROL DS

OPTIONS
RULEDEFS
RULEDEFB

SYSTEM EXITS

SMF EXITS
IEFU83 IEFU84
IEFU85

VSAM

Audited VSAM

Guardium Vulnerability Assessment

Based on best practices

- **Cost effectively improve the security of mainframe environments by conducting automated database vulnerability assessment tests**
  - Packaged tests to detect vulnerabilities including inappropriate privileges, grants, default accounts, etc..
  - Capabilities enabling the development of custom tests
- **Based on industry standards such as STIG and CIS**
- **Management of mainframe VA testing from central InfoSphere Guardium console for enterprise-wide control**
  - Configuration and scheduling of mainframe tests
- **Integrated with other InfoSphere Guardium elements for improved process efficiency, including Compliance Workflow Automation and audit repository**
- **Based on DB2 Development at SVL, DISA STIG and CIS security standards**
  - Server defaults
  - Patch levels
  - OS and DBMS Vulnerability Assessment

VA Report for DB2 on System z

IBM® InfoSphere™ Guardium®

Results for Security Assessment: **Assessment for DB2 on Z**

Assessment executed: **2011-12-02 04:15:16.0**
From: **2011-12-01 04:15:16.0**
To: **2011-12-02 04:15:16.0**

Tests passing:
*Percentage does

Based on the te
to learn how yo
improvement.

Result Summary — Showing 137 of 137 results (0 filtered)

	Critical			Major			Minor			Caution			Info		
Privilege	40p	14f	24e	4p	4f	--	--	--	--	--	--	--	--	--	--
Authentication	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Configuration	1p	1f	--	19p	15f	15e	--	--	--	--	--	--	--	--	--
Version	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Other	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Result Summary — Showing 137 of 137 results (0 filtered)

	Critical			Major			Minor			Caution			Info		
Privilege	40p	14f	24e	4p	4f	--	--	--	--	--	--	--	--	--	--
Authentication	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Configuration	1p	1f	--	19p	15f	15e	--	--	--	--	--	--	--	--	--
Version	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Other	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Current filtering applied:
Test Severities: - Show All -
Datasource Severities: - Show All -
Scores: - Show All -
Types: - Show All -

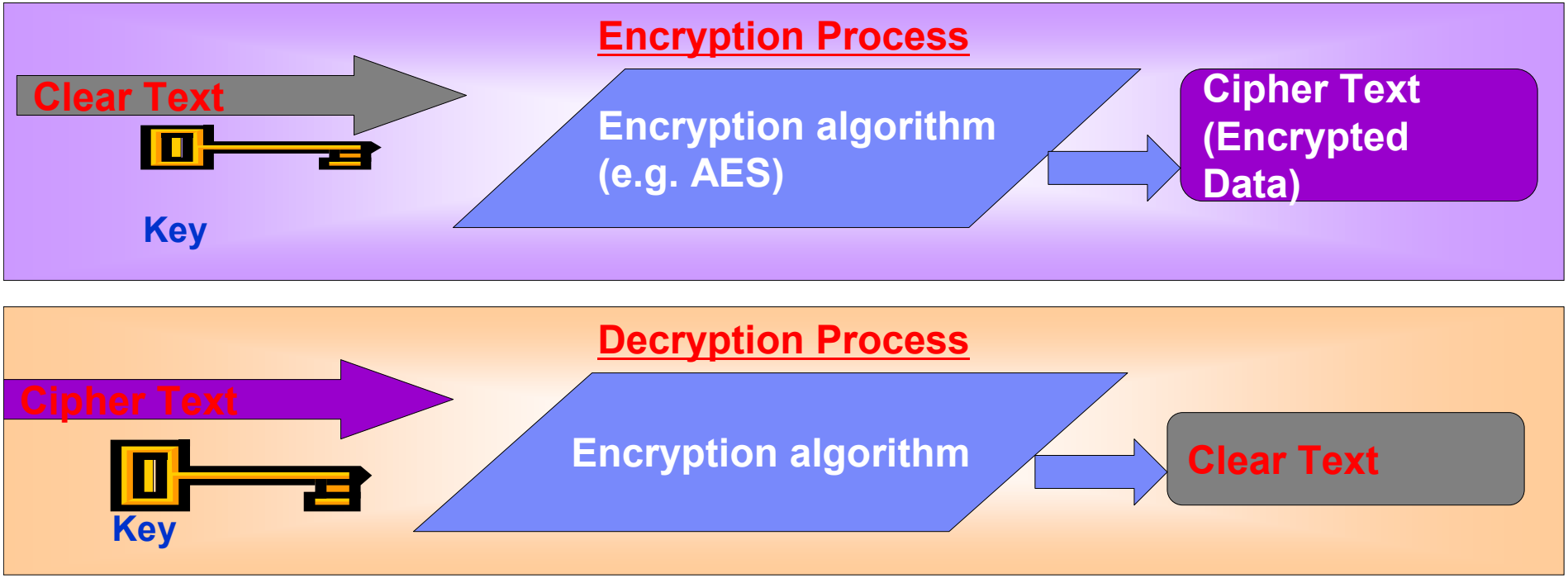
Assessment Test Results — Showing 137 of 137 results (0 filtered)

Test / Datasource	Result
z/OS Grant to PUBLIC - Package Test category: **Priv.** Severity: **Critical** This test check for object privileges on packages that has been granted to PUBLIC directly. We recommend user not granting objects privilege to PUBLIC. By default many objects are granted to PUBLIC and can be revoked. Ext. Reference: Guardium, Test ID 2170	**Fail** Packages privilege has been granted to PUBLIC. **Recommendation:** We recommend you revoke packages privilege from PUBLIC. For best practice, it is not good to grant any privilges to PUBLIC. If you need to exclude certain objects that must be granted to PUBLIC, you can create a group then populate it with authorize objects name and link your group to this test.

InfoSphere Guardium Value Propositions:

Proactive, Efficient & Effective Activity Response	Guardium provides full audit data collection processes with rules-based alerting that correlates abnormal/suspicious activity. These features will provide the maximum risk reduction across all mainframe data sources
Risk Reduction: Internal Privileged Users	Guardium monitoring cannot be evaded by any privileged user even those with Super Administrator IDs. Complete separation of duties ensures all activity is seen & alerted when anything suspicious happens in real-time.
Risk Reduction: Financial Crimes & Fraud Protection	Guardium provides full capability to audit any data used by any user. This audit info can be used for any fraud investigations. Guardium has the ability to audit end-users and audit what they viewed, selected, changed
Audit & Monitoring: Operational Effectiveness	Guardium provides auditors the ability to access the audit repository and with full authority to run reports and investigate any action. Can completely eliminate privileged user from the reporting process
Roadmap, Governance, Advanced Functionality	Regulations change each year requiring changes to mainframe auditing functionality and procedures. A significant data breach can occur at any time. Having a system to handle any future need is essential to success

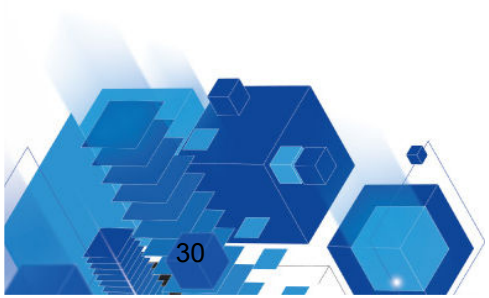
Encryption is a technique used to help protect data from unauthorized access



- Data that is not encrypted is referred to as “clear text”
- Clear text is encrypted by processing with a “key” and an encryption algorithm
  - Several standard algorithms exist, include DES, TDES and AES
- Keys are bit streams that vary in length
  - For example AES supports 128, 192 and 256 bit key lengths

InfoSphere Guardium Data Encryption for DB2 & IMS Databases

- Provides user-customizable EDITPROCs for DB2
- Works at the DB2 row level
- Provides user customizable segment edit exits for IMS
- Works at the IMS segment level
- Conforms to the existing z/OS security model
- Application Transparent
- Exploits zSeries Crypto Hardware features and corresponding Integrated Cryptographic Services Facility (ICSF) technologies, resulting in low overhead encryption/decryption



Example of a table without encryption - Rows accessed via SQL

```
 DB2 Admin -- DSNC BROWSE SYS248.UNENCRT          ------ Line 00000000 Col 001 080

******************************** Top of Data ********************************
 DEPTNO DEPTNAME
 ------ ------------------------------------------------------------------------
 007    CLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXT
 006    CLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXT
 005    CLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXT
 004    CLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXT
 003    CLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXT
 002    CLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXT
 001    CLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXT
 011    CLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXT
 010    CLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXT
 009    CLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXT
 008    CLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXT
******************************** Bottom of Data ********************************
```

External print of the tablespace container showing unencrypted table and clear text exposure of data

```
  Display  Filter  View  Print  Options  Search  Help
 ------------------------------------------------------------------------------------------------------------------------
 SDSF OUTPUT DISPLAY DB2PRINT JOB07373  DSID   101 LINE 37      COLUMNS 02- 133
 COMMAND INPUT ===>                                           SCROLL ===> CSR
PAGE: # 00000002 ------------------------------------------------------------------------------------------------------
DATA PAGE:  PGCOMB='00'X  PGLOGRBA='0052516AF000'X  PGNUM='00000002'X  PGFLAGS='00'X  PGFREE=77
            PGFREE='004D'X  PGFREEP=4003  PGFREEP='0FA3'X  PGHOLE1='0000'X  PGMAXID='07'X  PGNANCH=1
PGTAIL:  PGIDFREE='00'X  PGEND='E'
ID-MAP FOLLOWS:
01  024D 0014 0486 06BF 08F8 0B31 0D6A

RECORD:  XOFFSET='0014'X  PGSFLAGS='00'X  PGSLTH=569  PGSLTH='0239'X  PGSOBD='0006'X  PGSBID='02'X
F0F0F602 2EC3D3C5 C1D9E3C5 E7E3C3D3 C5C1D9E3 C5E7E3C3 D3C5C1D9 E3C5E7E3   006..CLEARTEXTCLEARTEXTCLEARTEXT
C3D3C5C1 D9E3C5E7 E3C3D3C5 C1D9E3C5 E7E3C3D3 C5C1D9E3 C5E7E340 40404040   CLEARTEXTCLEARTEXTCLEARTEXT
40404040 40404040 40404040 40C3D3C5 C1D9E3C5 E7E3C3D3 C5C1D9E3 C5E7E3C3                CLEARTEXTCLEARTEXTC
D3C5C1D9 E3C5E7E3 C3D3C5C1 D9E3C5E7 E3C3D3C5 C1D9E3C5 E7E3C3D3 C5C1D9E3   LEARTEXTCLEARTEXTCLEARTEXTCLEART
C5E7E340 40404040 40404040 40404040 40404040 40C3D3C5 C1D9E3C5 E7E3C3D3   EXT                    CLEARTEXTCL
C5C1D9E3 C5E7E3C3 D3C5C1D9 E3C5E7E3 C3D3C5C1 D9E3C5E7 E3C3D3C5 C1D9E3C5   EARTEXTCLEARTEXTCLEARTEXTCLEARTE
E7E3C3D3 C5C1D9E3 C5E7E340 40404040 40404040 40404040 40404040 40C3D3C5   XTCLEARTEXT                    CLE
C1D9E3C5 E7E3C3D3 C5C1D9E3 C5E7E3C3 D3C5C1D9 E3C5E7E3 C3D3C5C1 D9E3C5E7   ARTEXTCLEARTEXTCLEARTEXTCLEARTEX
E3C3D3C5 C1D9E3C5 E7E3C3D3 C5C1D9E3 C5E7E340 40404040 40404040 40404040   TCLEARTEXTCLEARTEXT
40404040 40C3D3C5 C1D9E3C5 E7E3C3D3 C5C1D9E3 C5E7E3C3 D3C5C1D9 E3C5E7E3        CLEARTEXTCLEARTEXTCLEARTEXT
C3D3C5C1 D9E3C5E7 E3C3D3C5 C1D9E3C5 E7E3C3D3 C5C1D9E3 C5E7E340 40404040   CLEARTEXTCLEARTEXTCLEARTEXT
40404040 40404040 40404040 40C3D3C5 C1D9E3C5 E7E3C3D3 C5C1D9E3 C5E7E3C3                CLEARTEXTCLEARTEXTC
D3C5C1D9 E3C5E7E3 C3D3C5C1 D9E3C5E7 E3C3D3C5 C1D9E3C5 E7E3C3D3 C5C1D9E3   LEARTEXTCLEARTEXTCLEARTEXTCLEART
C5E7E340 40404040 40404040 40404040 40404040 40C3D3C5 C1D9E3C5 E7E3C3D3   EXT                    CLEARTEXTCL
C5C1D9E3 C5E7E3C3 D3C5C1D9 E3C5E7E3 C3D3C5C1 D9E3C5E7 E3C3D3C5 C1D9E3C5   EARTEXTCLEARTEXTCLEARTEXTCLEARTE
```

Example of a table with encryption - Rows accessed via SQL and results presented to application requestor as cleartext

```
 DB2 Admin -- DSNC BROWSE SYS248.ENCRYPTB       ------ Line 00000000 Col 001 080

****************************** Top of Data ********************************
 DEPTNO DEPTNAME
 ------ ------------------------------------------------------------------
 007    CLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXT
 006    CLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXT
 005    CLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXT
 004    CLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXT
 003    CLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXT
 002    CLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXT
 001    CLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXT
 011    CLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXT
 010    CLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXT
 009    CLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXT
 008    CLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXTCLEARTEXT
****************************** Bottom of Data *****************************
```

Each SQL request will invoke the EDITPROC and result in cleartext being presented back to any *AUTHORIZED* requestor

External print of the tablespace container showing encrypted table and Cybertext data without exposure of data

```
  Display  Filter  View  Print  Options  Search  Help
 ------------------------------------------------------------------------------------------------
 SDSF OUTPUT DISPLAY DB2PRINT JOB07385  DSID   101 LINE 37      COLUMNS 02- 133
 COMMAND INPUT ===>                                          SCROLL ===> CSR
PAGE: # 00000002 ------------------------------------------------------------------------------
DATA PAGE:  PGCOMB='10'X  PGLOGRBA='0052516DC2A5'X  PGNUM='00000002'X  PGFLAGS='00'X  PGFREE=77
           PGFREE='004D'X  PGFREEP=4003  PGFREEP='0FA3'X  PGHOLE1='0000'X  PGMAXID='07'X  PGNANCH=7
PGTAIL:  PGIDFREE='00'X  PGEND='N'
ID-MAP FOLLOWS:
01  0014 024D 0486 06BF 08F8 0B31 0D6A

RECORD:  XOFFSET='0014'X  PGSFLAGS='00'X  PGSLTH=569  PGSLTH='0239'X  PGSOBD='0009'X  PGSBID='01'X
7F303398 CC9173EA 10472451 F7EA1E11 E90937CE AB19878B 6697669A 6453B49D   "...........7...Z.............
59F24AD6 6744E8A8 C89B51CB 8900AA9A E918B1C7 706F8D1C A936D79D E6FF4659   .2.O..Y.H.......Z..G.?....P.W...
8D57E65B AEB8AE9D C915C5D6 4E20555B 4E6864D5 C6F727BB 018CFF75 CC0E8FD6   ..W$....I.EO+..$+..NF7.........O
B033B100 A0E82ECF C24D3369 1A680C70 DCF1AE71 54E81B0A 6729A7D3 B6927139   .....Y..B(.......1...Y.....L....
4D3A2052 44BDFA4F 01E0B441 86F5F133 970DE3F7 1B731133 92350E3C 3B430DB6   (.....|.....51...T7............
E60C9620 DE155654 4DC94A02 FF292FB8 000C6C94 B0C5B870 FAECF085 D0B7FD84   W.......(I........%..E....0.....
5FB867CB 21A47CFC F5F500EB 3FD8DD83 35C7C50E 50680098 C61E92F8 C0D0F683   ¬.....@.55...Q...GE.&...F..8..6.
36526B43 F79A945F 70FE4BA5 FFBD6D2A 9350D5C8 7279675D 799C6DB2 E475CD12   ..,.7..¬......_..&NH...)..._.U...
CB600124 759CE537 E516E74E F0A0BF0A BF0D19AA 2CD1A351 D353D496 07E61341   .-....V.V.X+0........J..L.M..W..
3A0F4D90 810B44BF 9952BAA5 8365841E CEE2A45E E820D13D 33E2E991 C8D51E6F   ..(.............S..Y.J..SZ.HN.?
448A282F A32AF20B 7E364706 164E4A8C CD499F7C 62902023 9FF5C2DA B25BA1A3   ......2.=....+.....@.....5B..$..
F8A1B6BD 02CC1A1C 270C3B1E 2EC7CD35 C34014DA 45D122B2 5DC8702B 933FEC8C   8...........G..C ...J..)H......
C07A832A 086C4D8D 305055C1 33EDCE56 E7E0488A FAEAFD33 EBAC3373 C3A4D0EC   .:...%(..&.A....X...........C...
B7BCDF34 FD87142E 3E4592B7 63927E0D 0582B935 560DEF54 CC126994 6B84B7FB   .............=.............,...
F0104C9E EDE08F00 D18C336A 9E89FDF6 359CF675 F717C33F AA32EE54 32C1FC63   0.<.....J......6..6.7.C......A..
```

InfoSphere Guardium Data Encryption for DB2 and IMS Databases

- Existing implementation uses DB2 EDITPROC for row level encryption
  - Application Transparent
  - Acceptable overhead when accessing any column in table
  - No Additional Security
  - Table must be dropped and reloaded to add EDITPROC
  - Indexes not encrypted
- New Functionality User Defined Function (UDF) for column level encryption
  - Requires changes to SQL when accessing encrypted column
  - High overhead when accessing encrypted column, no overhead on non-encrypted columns
  - Can secure UDF in RACF for additional security
  - Index Encryption
  - Data encrypted in place
  - Implementation can be less disruptive that other approaches (SQL based)
  - See document at: http://www-01.ibm.com/support/docview.wss?uid=swg21586761&aid=1

ibm.com/guardium