



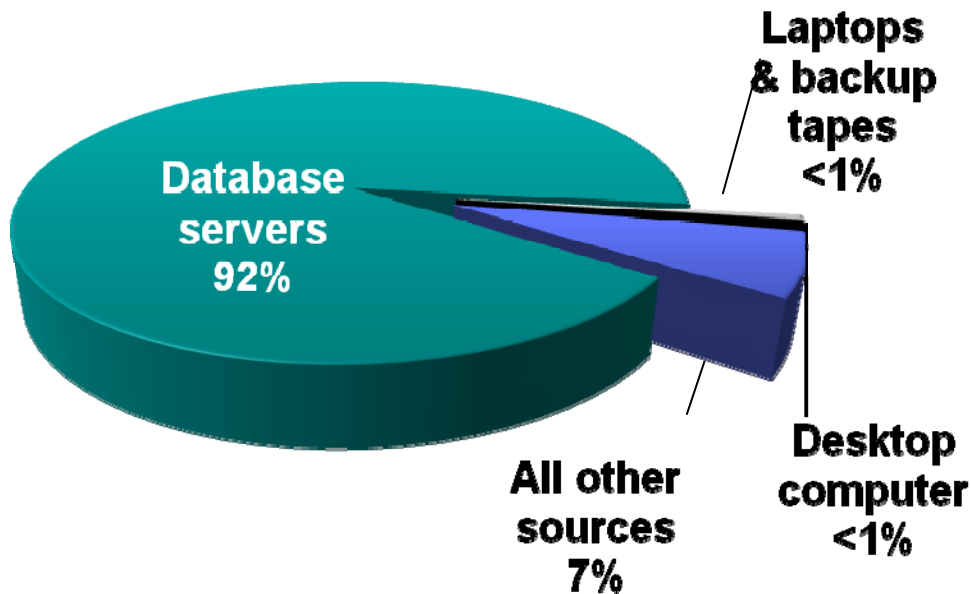
A proactive approach to security, audit and compliance on DB2 for z/OS



Database Servers

The Primary Source of Breached Data

% of Records Breached (2010)



...up from 75% in 2009

“Although much angst and security funding is given to offline data, mobile devices, and end-user systems, these assets are simply not a major point of compromise.”

- 2009 Data Breach Investigations Report

Why?

- **Database servers contain your most valuable information**
 - Financial records
 - Customer information
 - Credit card and other account records
 - Personally identifiable information
- **High volumes of structured data**
- **Easy to access**



“Because that’s where the money is.”

- Willie Sutton

Database Danger from Within

- “Organizations overlook the most imminent threat to their databases: authorized users.” (Dark Reading)
- “No one group seems to own database security ... This is not a recipe for strong database security” ... 63% depend primarily on manual processes.” (ESG)
- Most organizations (62%) cannot prevent super users from reading or tampering with sensitive information ... most are unable to even detect such incidents ... only 1 out of 4 believe their data assets are securely configured (Independent Oracle User Group).

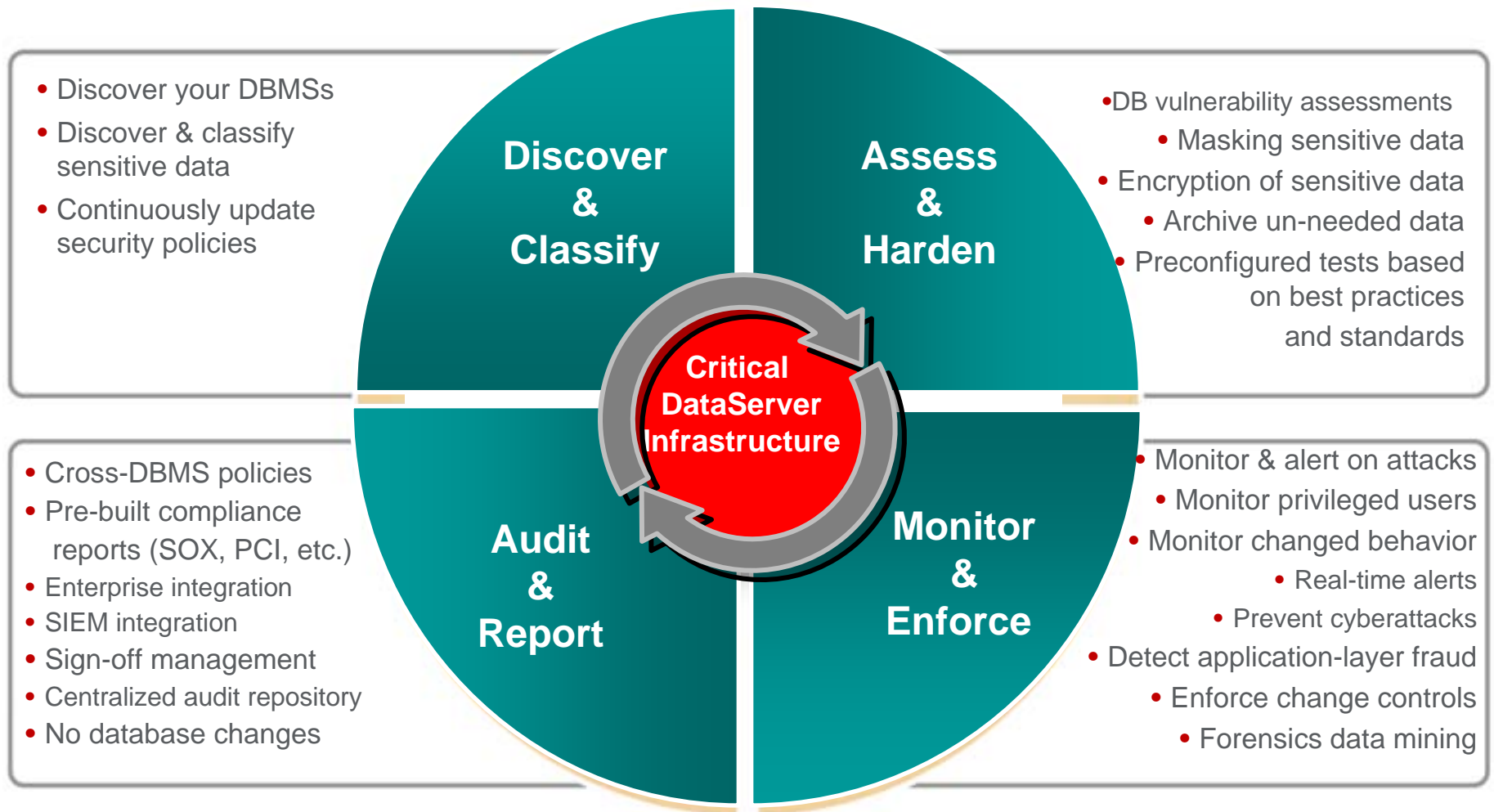


Growing Compliance Mandates



- **Explosion in successful breaches has resulted in growing regulation of sensitive data in North America**
 - SOX
 - HIPAA
 - PCI DSS
 - 46 state-specific data privacy laws
 - Gramm-Leach-Bliley
- **Many EU and Asian countries have enacted similar regulations**
 - EU Data Privacy Directive and supporting local laws
 - C-SOX
 - FIEL
 - PCI DSS
 - etc.

Address the Full Data Protection Lifecycle



DB2 10 - Better Protection and Auditing capability

■ Improved Access Controls

- Minimize the need for super-user authorities such as SYSADM
- New authorities with no access to data
- Improved separation of duties
 - System Administrators
 - Database Administrators
 - Security Administrators

■ Improved Data Auditing

- Any dynamic access or use of a privileged authority needs to be included in your audit trail
- Maintain historical versions of data for years or during a business period

■ Improved Data Privacy

- All dynamic access to tables containing restricted data needs to be protected



*Today's Mainframe:
The power of industry-leading security,
the simplicity of centralised management*

New DB2 10 granular database and security authorities

Prior to DB2 10

- SYSADM
- DBADM
- DBCTRL
- DBMAINT
- SYSCTRL
- PACKADM
- SYSOPR

New in DB2 10

- System level DBADM authority
 - Granted with or without ACCESSCTRL
 - Granted with or without DATAACCESS
- System level SECADM authority
- System level SQLADM authority
- Application level EXPLAIN privilege



New DB2 10 fine grain table controls

Protect against unplanned SQL access



- **Define additional table controls at the row and column level**
 - Security policies are defined using SQL
 - Separate security logic from application logic
- **Security policies based on real time session attributes**
 - Protects against SQL injection attacks
 - Determines how column values are returned
 - Determines which rows are returned
- **No need to remember various view or application names**
 - No need to manage many views; no view update or audit issues
- **Mask column values in answer set**
- **All access via SQL including privileged users, adhoc query tools, report generation tools is protected**
- **Policies can be added, modified, or removed to meet current company rules without change to applications**

New DB2 10 Audit Policies

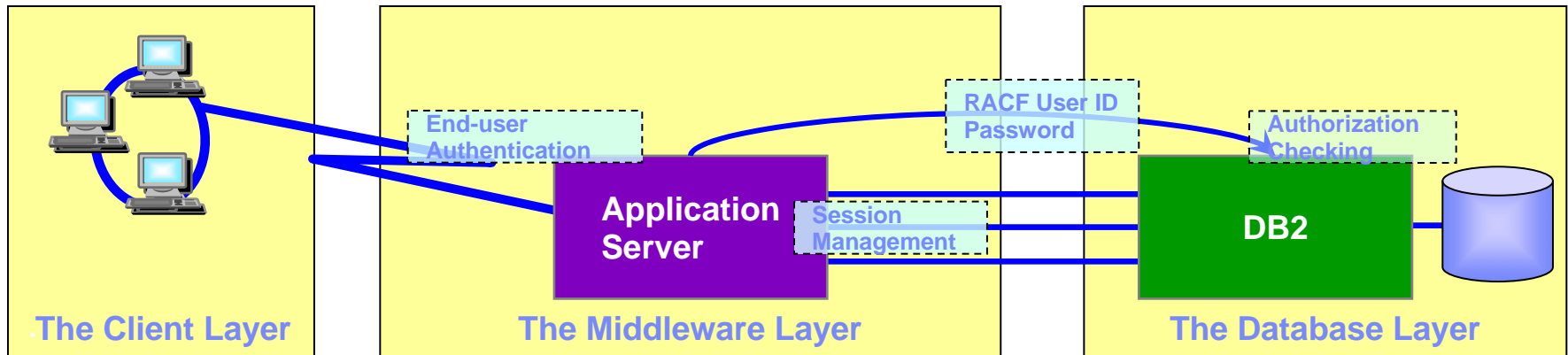
Provides needed flexibility and functionality

- **Auditor can audit access to specific tables for specific programs during day**
 - Audit policy does not require AUDIT clause to be specified using DDL to enable auditing (no more DBA involvement and no package invalidation)
 - Audit policy generates records for all read/update access, not just first access
 - Audit policy includes additional records identifying the specific SQL statements
 - Audit policy provides wildcarding of based on schema and table names
- **Auditor can identify any unusual use of a privileged authority**
 - Records each use of a system authority
 - Audit records written only when authority is used for access
 - External collectors only report users with a system authority



DB2 Identity Amnesia

An example of a typical application server security model



- **In a typical application server model, the middle layer:**
 - authenticates end-users running client applications
 - manages all interactions with DB2
- **Application server then uses a common RACF User ID and password to authenticate and authorize connections to DB2**
- **Common user ID is then used for DB2 authorization on behalf of all end-users**
- **DB2 10 features can be used to eliminate this kind of exposure by:**
 - Enabling RACF client certificate authentication to protect the RACF User ID
 - Enabling DB2 trusted context to exploit role authorization
 - Enabling DB2 trusted context to exploit RACF distributed identity propagation

DB2 10 synergy with recent z/OS security features

- **Support distributed identities introduced in z/OS V1R11**
 - A distributed identity is a mapping between a RACF user ID and one or more distributed user identities, as they are known to application servers
- **Support client certificates authentication in z/OS V1R10**
 - Client certificate be registered with RACF (or other SAF compliant security product) and mapped to a user ID
- **Support password phrases introduced in z/OS V1R10**
 - Password phrase is a character string made up of mixed-case letters, numbers, special characters, and is between 9 to 100 characters long
- **Support connection level security enforcement**
 - Enforces connections must use strong authentication to access DB2
 - All userids and passwords encrypted using AES, or connections accepted on a port which ensures AT-TLS policy protection or protected by an IPSec encrypted tunnel

RACF and Data Servers on z/OS

▪ RACF and DB2

- DB2 Subsystem Access Control (outside of DB2)
- Control connections to the DB2 subsystem
 - CICS
 - IMS
 - CAF
 - BATCH
- Assign identities
- Protect the underlying DB2 data store (underlying data sets of DB2 can be protected by RACF dataset services)
- In addition to database server-provided security, RACF can be used to control access to database objects, authorities, commands and utilities by using the RACF access control module of the database server.

Tools from Security to enhance RACF

▪ **Security zSecure Admin**

- User friendly layer over the native RACF administration panels
- Automatically generated RACF commands
 - Reduce complexity
 - Increased RACF administration productivity
 - Fewer errors
 - Less risk of inadvertent data exposure due to inappropriate/insufficient security

▪ **Security zSecure Visual**

- GUI/Windows based UI
- Insulates security administrators from TSO/ISPF
- Increased productivity requiring less sophistication in administration skills

▪ **Security Identity Management software**

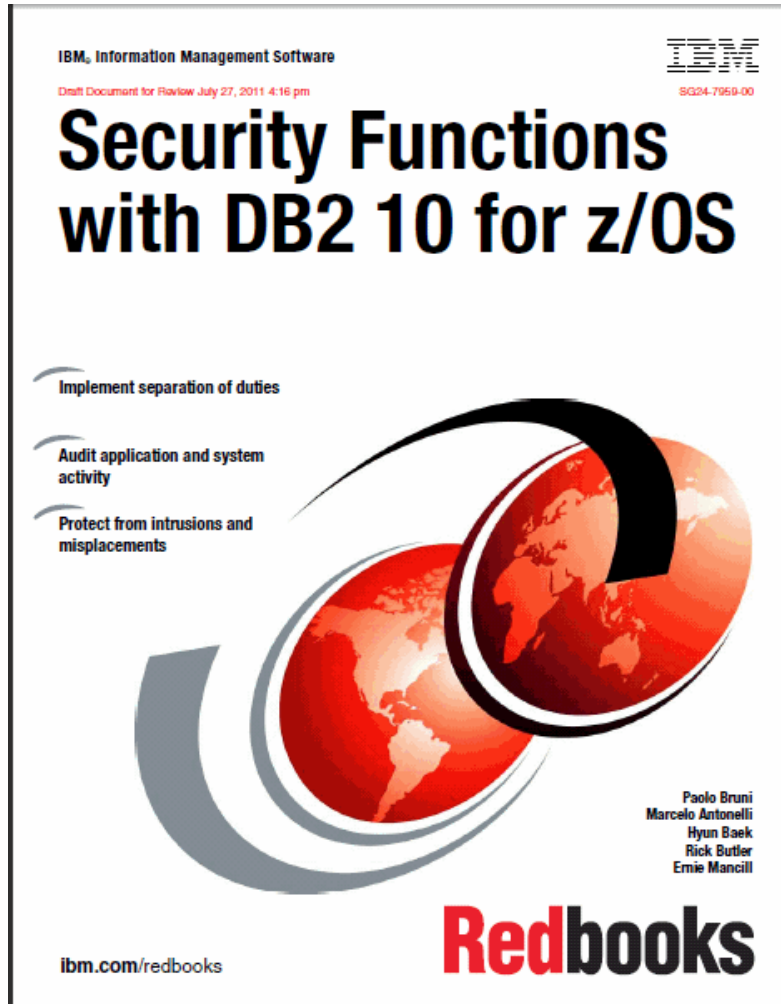
- Security Directory Server
- Security Identity Manager

DB2 10 provides new ways to satisfy auditors

- ✓ New controls to prevent data access outside your trusted applications
- ✓ New granular authorities to reduce data exposure of administrators
- ✓ New auditing features using new audit policies used to comply with new laws
- ✓ New row and column access table controls to safe guard all access to your data
- ✓ New temporal data to comply with regulations to maintain historical data



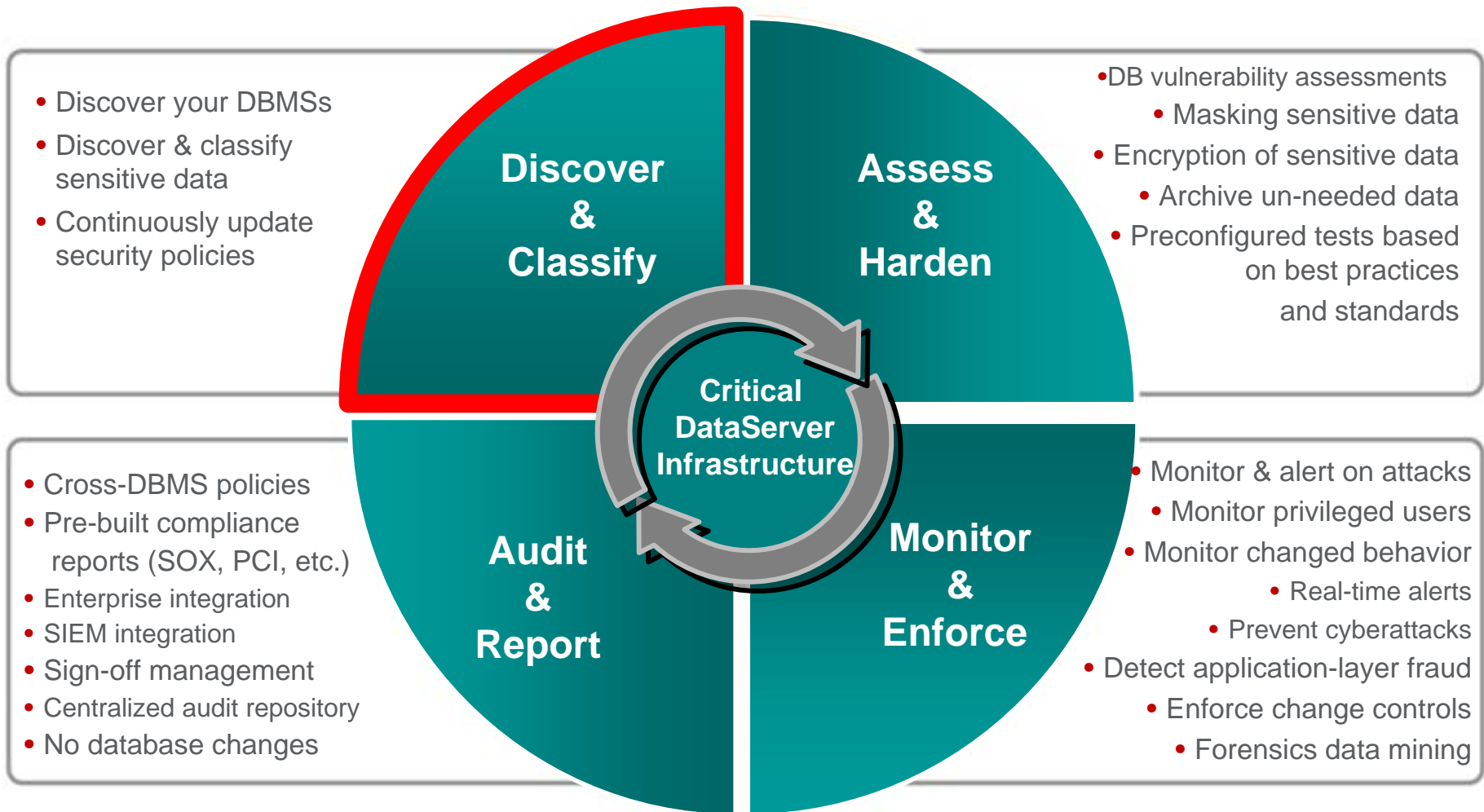
New security Redbook now available on www.redbooks.ibm.com



Topics covered include:
Governance and Information Protection
DB2 V10 Security Enhancements:
 SECADM for separation
 Row permissions
 Temporal Support
 Auditing
Encryption on z/OS
Guardium for z/OS

SG24-7959

Address the Full Data Protection Lifecycle



Find your Data Servers (with Guardium)

- Scan the network to develop an inventory of databases
- Schedule regular scans to discover new instances
- Policy-based actions
 - Alerts
 - Add to group for monitoring

Administration Console | Access Management | Tools | Daily Monitor | SQL Guard Monitor | Tap Monitor | Incidents

SQL Count
Session Count
Logged Threshold Alerts
Logged R/T Alerts
Exception Count
Dropped Requests
TCP Exceptions
Admin User Logins
Databases by Type
Databases Discovered
Retrospective Report Requests
Values Changed
Throughput

Databases Discovered

Start Date: 2008-06-26 14:48:49 End Date: 2008-06-26 15:48:49

<u>Time Probed</u>	<u>Server IP</u>	<u>Server Host Name</u>	<u>DB Type</u>	<u>Port</u>	<u>Port Type</u>	<u>#</u>
2008-06-26 15:31:00	10.10.9.253	10.10.9.253	Oracle	1521	tcp	1
2008-06-26 15:30:58	10.10.9.253	10.10.9.253	MSSQL	1433	tcp	1
2008-06-26 15:30:15	10.10.9.55	osprey	Oracle	1521	tcp	1
2008-06-26 15:30:15	10.10.9.55	osprey	Sybase	4200	tcp	1
2008-06-26 15:30:32	10.10.9.56	10.10.9.56	Oracle	1521	tcp	1
2008-06-26 15:30:58	10.10.9.56	10.10.9.56	DB2	50001	tcp	1

(Big problem on LUW, less interesting on z?)

Identify Sensitive Data

Why is Sensitive Data Discovery so Data Difficult?

Sensitive Relationship Discovery

System A Table 1		System A Table 15		
Number	Name	Patient	Result	Test
3544600986	AlexFulltheim	3802468	N	53
5728150928	BarneySolo	4182715	N	53
3786736304	BillAlexander	4600986	N	32
6783802468	BobSmith	5061085	N	53
4035567193	EileenKratchman	5567193	N	72
8037409934	FredSimpson	6123913	Y	47
4306123913	George Brett	6736304	N	34
9525061085	JamieSlattery	7409934	N	34
4594182715	JimJohnson	8150928	N	47
1288966020	MartinAston	8966020	N	34

System Z Table 25	
Test	Name
53	Streptococcus pyogenes
72	Pregnancy
32	Alzheimer Disease
47	Hemorrhoids
34	Dermatamycoses

- **Sensitive data can't be found just by a simple data scan.**
 - Must connect tables and lookup tables
 - Hidden within larger fields (substring)
 - Hidden across fields (concatenations)
 - Represented differently (lookup tables and case statements)

- **“Corporate memory” is poor**
 - Documentation is incomplete
 - SME's and Data Analysts are only knowledgeable of one or two systems
 - Proprietary data model with vendor products

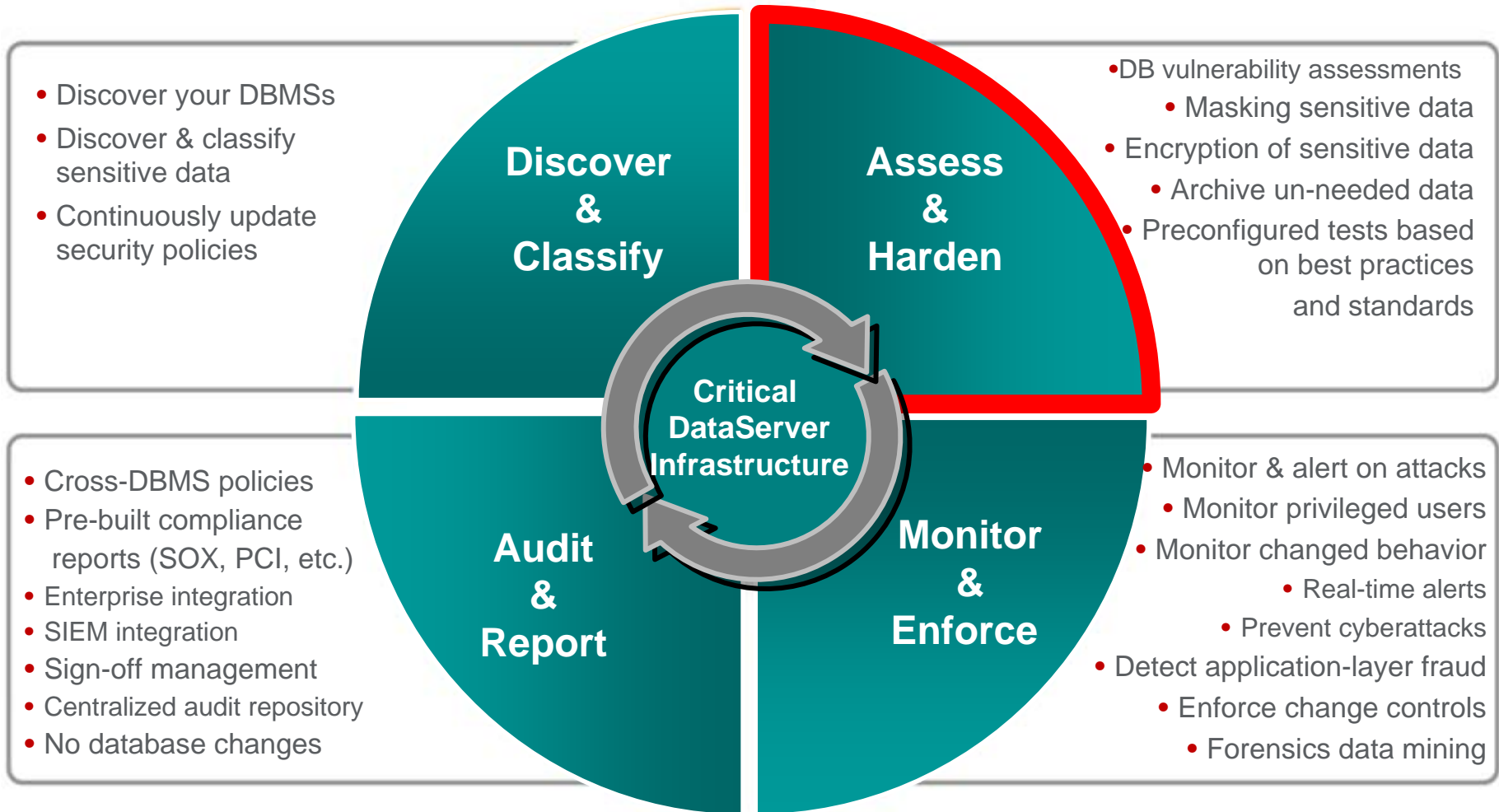
- **Hundreds of tables and millions of rows:**
 - Complex
 - Difficult to verify

- **Data quality problems make discovery even more difficult**

Sensitive Data Discovery - InfoSphere Discovery

- **Common PII data element discovery**
 - Pre-Defined Scanning
- **Custom sensitive data discovery**
 - Supply Discovery with “descriptions/examples”
 - *Patterns*
 - *Data examples.*
 - Discovery will scan for matching columns
- **Hidden sensitive data discovery**
 - Sensitive data embedded in free text columns
 - Scan by “floating” patterns
 - Sensitive data that is partial or hidden
 - Use Transformation Discovery to find data that are “transformed”

Address the Full Data Protection Lifecycle



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 and passwords, security exposures, patches, 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

Results for Security Assessment: **VA test for system Z**

Assessment executed **2010-09-20 13:55:27.0**
 From: **2010-09-19 13:55:27.0**
 To: **2010-09-20 13:55:27.0**
 Client IP or IP subnet: **Any**
 Server IP or IP subnet: **Any**

Tests passing: **88%***

*Percentage does not take into account any current filtering

Based on the tests performed under this assessment, data access of the defined database environments conform to best practices. You have a controlled environment in terms of the tests performed. You should consider scheduling this assessment as an audit task to continuously assess these environments.



Result Summary Showing 73 of 73 results (0 filtered)

	Critical	Major	Minor	Caution	Info
Privilege	46p 4f	7p 1f			
Authentication					
Configuration	1p				
Version		1p			
Other	1p	3p 2f	2p 1f		3p 1f

Current filtering applied:

- Test Severities: - Show All -
- Datasource Severities: - Show All -
- Scores: - Show All -
- Types: - Show All -

Assessment Test Results

Showing 73 of 73 results (0 filtered)

Test / Datasource	Result
z/OS Grant option - Resauth Test category: Priv. Severity: Critical This test check for privileges on various resources that has been granted with the grant option. These resource include: Buffer pool, Collection, Distinct type, Table space, Storage group and JAR file. Grant option is not a good practice and should be avoid where possible. When privileges are granted with the grant option, a user can grant privileges on that resource to other users. We do not recommend granting resource privilege with grant option. This test exclude grantee who is a member of SYSADM and SYSIBM user. Ext. Reference: Guardium, Test ID 2179	Fail One or more resources privileges has been granted with the grant option. Recommendation: We recommend that you revoke resources privileges granted with the grant option. Please redo your resource privilege so that you are using grant instead of grant option. If you need to exclude certain grantee or resource that must have grant option, you can create a group then populate it with authorize grantee and or resource name and link your group to this test.
System Z Datasource Datasource type: DB2 Severity: None Details: Grantee causing failure: Grantee=ADMIN_A: Otype=D: Qualifier=GU0003: Name=CANADIAN_DOLLAR Grantee=ADMIN_A: Otype=D: Qualifier=GU0002: Name=CANADIAN_DOLLAR	
z/OS Grant option - Schema Test category: Priv. Severity: Critical This test check for schema privileges that has been granted with the grant option. Grant option is not a good practice and should be avoid where possible. When object privileges are granted with the grant option, a user can grant privileges on that object to other users. We do not recommend granting objects privilege with grant option. This test exclude grantee who is a member of SYSADM and SYSIBM user. Ext. Reference: Guardium, Test ID 2181	Fail One or more object privileges has been granted with the grant option. Recommendation: We recommend that you revoke schema privileges granted with the grant option. Please redo your schema privilege so that you are using grant instead of grant option. If you need to exclude certain grantee or objects that must have grant option, you can create a group then populate it with authorize grantee and or objects name and link your group to this test.

IBM InfoSphere Guardium: Security Assessment Results - Mozilla Firefox

9.70.147.47 https://9.70.147.47:8443/saResultsViewer.do?method=view&viewerType=testResultDetails&viewedTaskId=-1&selectedTestResultId=20158&saResultId=20001

IBM® InfoSphere™ Guardium®

Results for Security Assessment: **VA test for system Z**

Assessment executed **2010-09-20 13:55:27.0**
 From: **2010-09-19 13:55:27.0**
 To: **2010-09-20 13:55:27.0**

Client IP or IP subnet: **Any**
 Server IP or IP subnet: **Any**

Test Result History

z/OS Grant option - Resauth
 Test category: **Priv.** Test severity: **Critical**

System Z Datasource
 Datasource type: **DB2** Datasource severity: **None**

Fail

One or more resources privileges has been granted with the grant option.

Short Description: This test check for privileges on various resources that has been granted with the grant option. These resource include: Buffer pool, Collection, Distinct type, Table space, Storage group and JAR file. Grant option is not a good practice and should be avoid where possible. When privileges are granted with the grant option, a user can grant privileges on that resource to other users. We do not recommend granting resource privilege with grant option. This test exclude grantee who is a member of SYSADM and SYSIBM user.

External Reference: Guardium, Test ID 2179

Recommendation: *We recommend that you revoke resources privileges granted with the grant option. Please redo your resource privilege so that you are using grant instead of grant option. If you need to exclude certain grantee or resource that must have grant option, you can create a group then populate it with authorize grantee and or resource name and link your group to this test.*

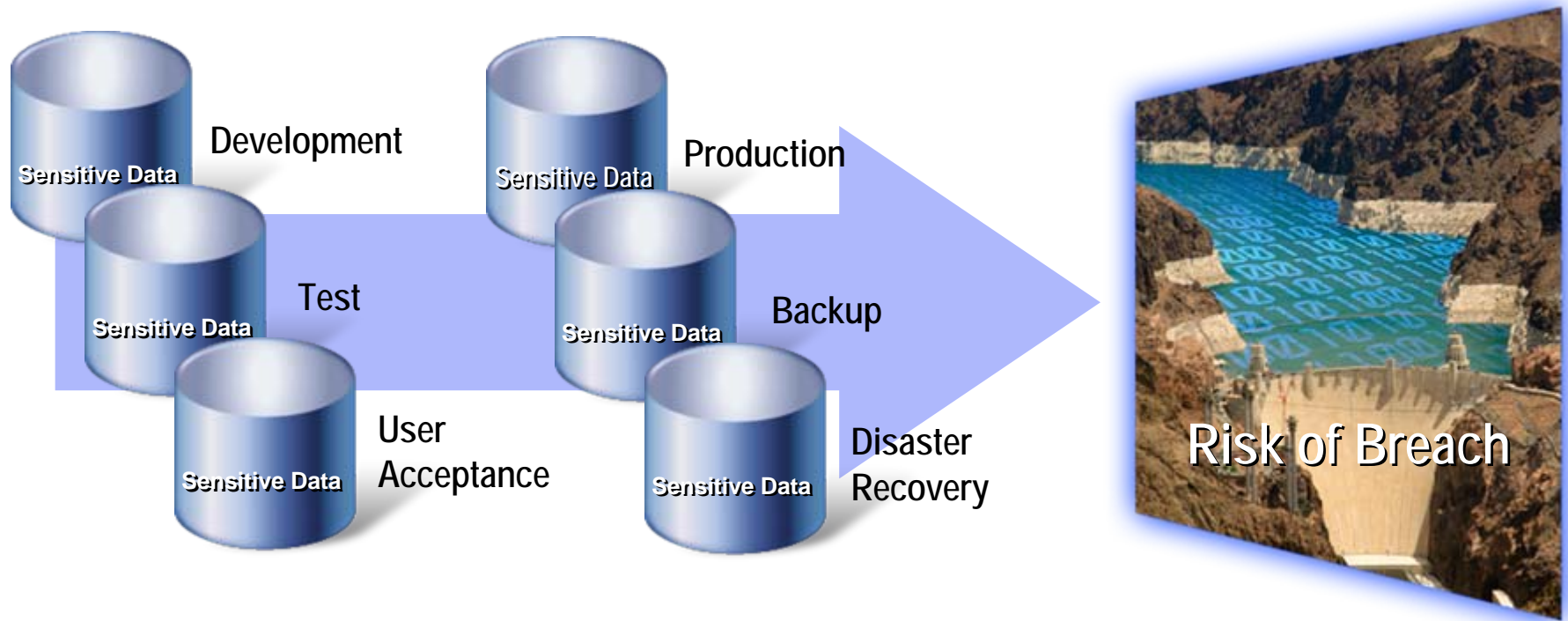
Details: Grantee causing failure: Grantee=ADMIN_A; Obtype=D; Qualifier=GU0003; Name=CANADIAN_DOLLAR
 Grantee=ADMIN_A; Obtype=D; Qualifier=GU0002; Name=CANADIAN_DOLLAR

[Close this window](#)

Done

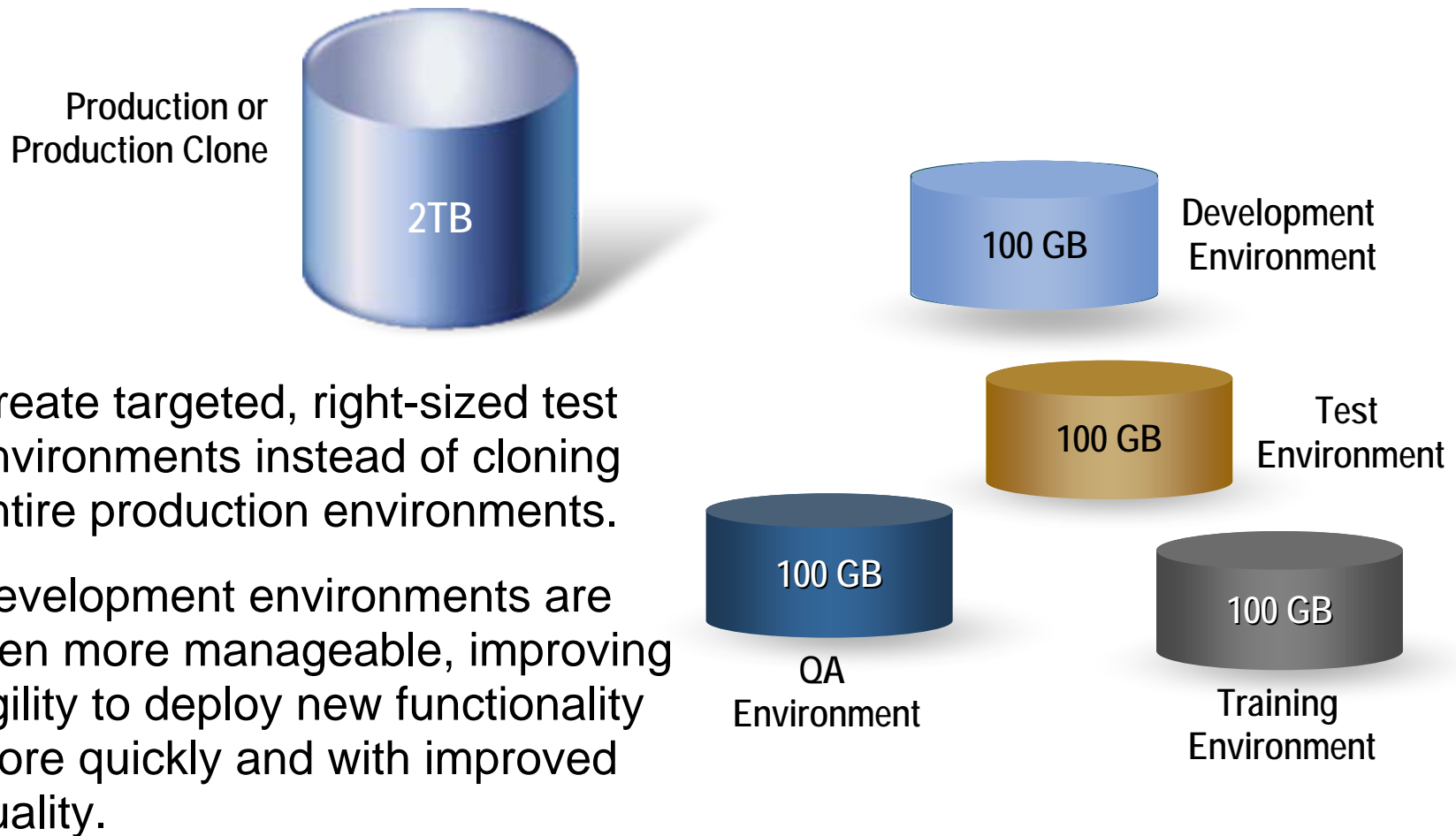
Limit the scope of compliance and security concerns

Sensitive Data Proliferation



**Actual risk and compliance burden =
Original production data + all derived clones**

Effective Test Data Management



OPTIM Test Data Management

Sensitive Data Masking

OPTIM Data Privacy

Masked or transformed data must be appropriate to the context:

- Consistent formatting (alpha to alpha)
- Context and application aware
- Within permissible range of values
- Maintain referential integrity

A comprehensive set of data masking techniques to transform or de-identify data, including:

- String literal values
- Character substrings
- Random or sequential numbers
- Arithmetic expressions
- Concatenated expressions
- Date aging
- Lookup values
- TRANS COL

Example 1

Patient Information			
Patient No.	123456	SSN	333-22-4444
Name	Erica Schafer		
Address	12 Murray Court		
City	Austin	State	TX Zip 78704

Data is masked with contextually correct data to preserve integrity of test data

Example 2

Personal Info Table		
PersNbr	FirstName	LastName
10000	Jeanne	Renoir
10001	Claude	Monet
10002	Pablo	Picasso
	⋮	

Referential integrity is maintained with key propagation

Event Table		
PersNbr	FstNEvtOwn	LstNEvtOwn
10002	Pablo	Picasso
10002	Pablo	Picasso

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
- Exploits zSeries Crypto Hardware features and corresponding Integrated Cryptographic Services Facility (ICSF) technologies, resulting in low overhead encryption/decryption



InfoSphere Guardium Data Encryption for DB2 and IMS

- **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 encryption**
 - Requires changes to SQL when accessing encrypted column
 - Higher 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 than other approaches (SQL based)
- **More functionality planned in future product enhancements**

Encryption hardware support on zSeries

- **CEX3C**
 - FIPS 140-2 Level 4 compliant tamper resistance hardware
 - Cryptographic Hardware Coprocessor or SSL Accelerator
- **DS8000 Encrypting Disks**
 - Implemented by storage subsystem
- **TS Encrypting Tape Drives**
- **Enterprise Key Management**
 - ISKLM

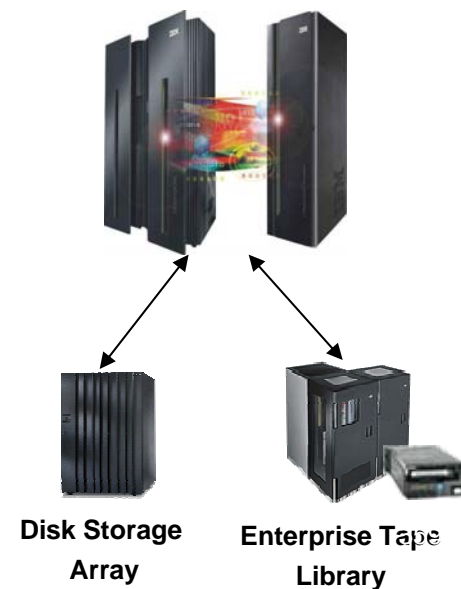
Security Key Lifecycle Manager for z/OS V1.1

Attributes of encryption and key management:

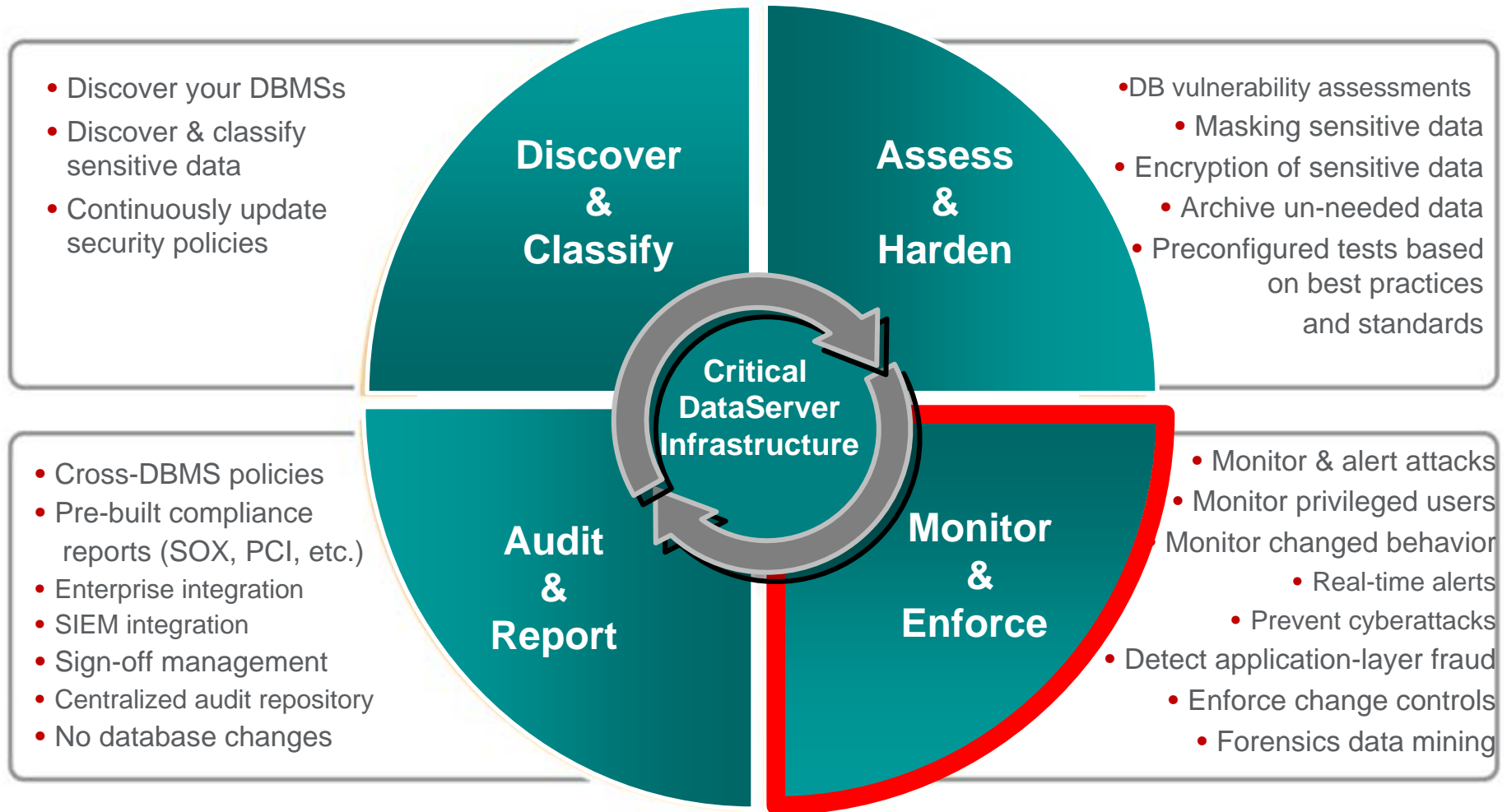
- Encryption in storage hardware does not hurt performance
- Encryption and key management doesn't require changing applications, middleware, JCL, operating systems
 - Key management completely separate from the data path
 - Storage arrays and libraries contact the key manager on behalf of the application and hosts doing I/O
 - With disk arrays done at power up
 - With tape libraries at each cartridge mount
- Encryption and key management fits into your operations management
 - Separation of duties
 - Leverage investments in high availability and security

ISKLM V1.1 benefits:

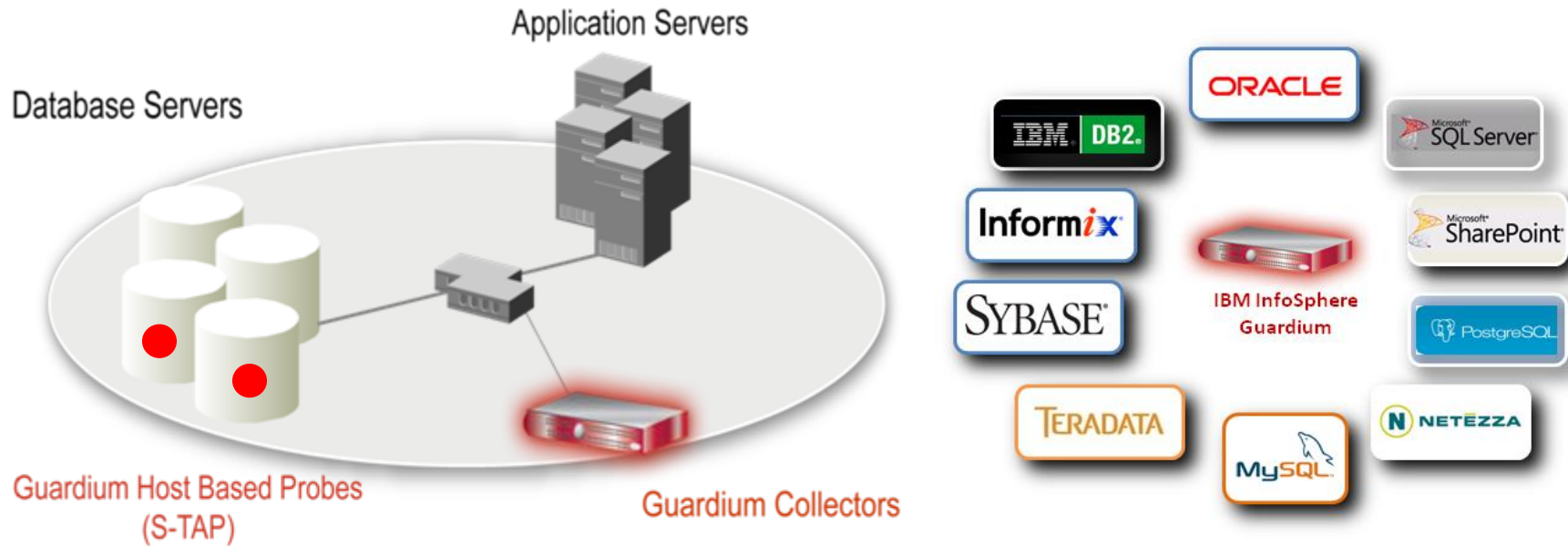
- Easy upgrade from EKM, easy SMPE install
- Still supports ICSF, RACF, crypto express hardware
- Writes SMF records type 83 subtype 6
- Supports all of the latest system z centric storage – tape and disk
- No longer requires DB2 or SSRE



Address the Full Data Protection Lifecycle



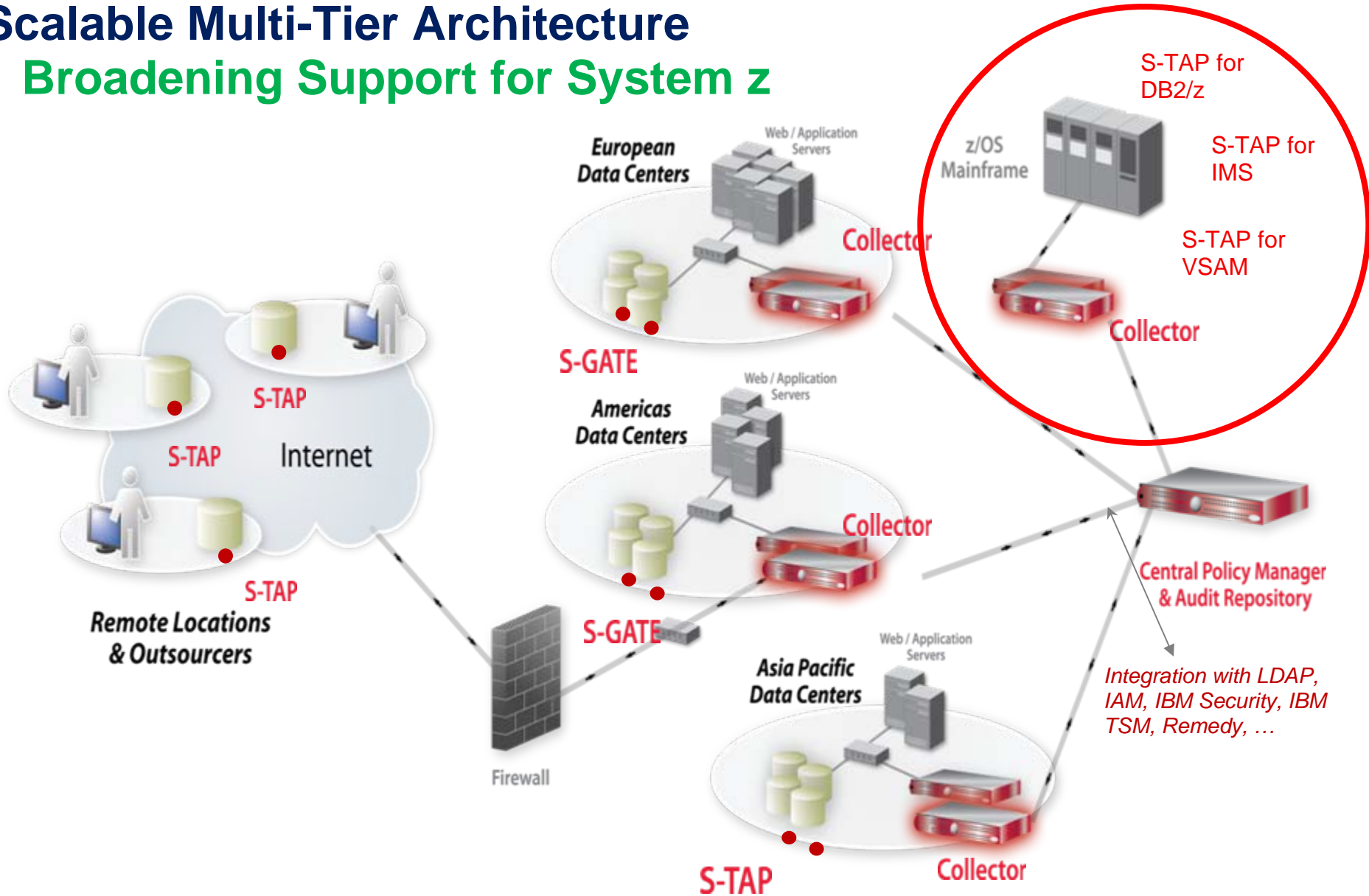
Monitor and Enforce – Database Activity Monitoring



- Non-invasive architecture
 - Outside database
 - Minimal performance impact
 - No DBMS or application changes
- Cross-DBMS solution
- 100% visibility including local DBA access
- Enforces separation of duties
- Does not rely on DBMS-resident logs that can easily be erased by attackers, rogue insiders
- Granular, real-time policies & auditing
 - *Who, what, when, how*
- Automated compliance reporting, sign-offs & escalations (SOX, PCI, NIST, etc.)

Scalable Multi-Tier Architecture

Broadening Support for System z



Guardium for z - Components

- **Guardium Collector appliance for System z**
 - Securely stores audit data collected by mainframe tap
 - Hardened Linux kernel, no root access possible
 - Secure Audit repository with no native database access
 - Access via Web browser GUI
 - Provides analytics, reporting & compliance workflow automation
 - Integrated with Guardium enterprise architecture
 - Centralized, cross-platform audit repository for enterprise-wide analytics and compliance reporting across mainframe & distributed environments
 - S-TAP for DB2 on z/OS event capture
- **Mainframe probe (runs as z/OS STC's)**
 - Collects audit data for Guardium appliance
 - Collection profiles managed on the Guardium appliance
 - Extensive filtering available to optimize data volumes and performance
 - Enabled for zIIP processing
 - All data streamed to appliance – small mainframe footprint
 - DB2 trace not used for high volume SQL events



Guardium for z – Mainframe Integration

Guardium appliance in zBX

New form factor for the Guardium appliance

Appliance runs inside zBX mainframe blade extender on x-series blades

Consistent system management of resources across mainframe

Dynamic allocation of linux capacity on blades for Guardium

Internal dedicated network between S-TAP on z/OS and zBX appliance



Guardium S-TAP for IMS on z/OS - New 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 VSAM on z/OS - New Product

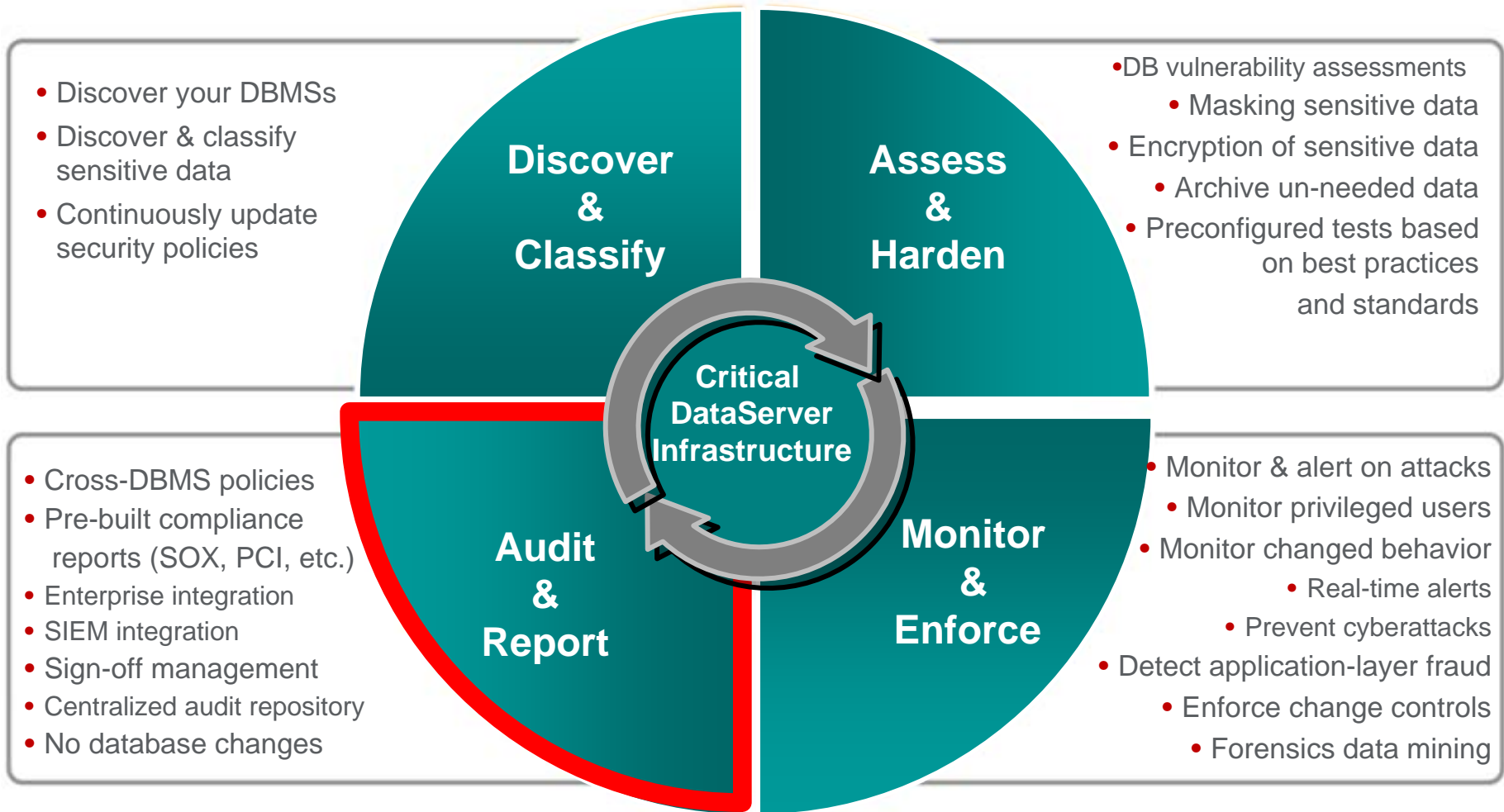
Monitor access to sensitive data in VSAM datasets

Monitoring datasets related to the DBMS

Monitor access to DB2 VSAM LDS containers that bypass 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


Address the Full Data Protection Lifecycle




Audit and Report

Custom and Pre-Built Compliance Reports





- Custom reporting
- SOX and PCI accelerators
 - Financial application monitoring (EBS, JD Edwards, Peoplesoft, etc)
 - Authorized application access only
 - Automated compliance reporting, sign-offs & escalations (SOX, PCI, NIST, etc.)

PCI Accelerator 

Overview | REG 3 Protect  | REG 6 Maintain | REG 7 Restrict | REG 8 Assign | PCI Req. 10 Track & Monitor | REG 11 Test | PCI Policy Monitoring

Overview

- Cardholder Server IPs List
- Cardholders DBs
- Cardholder Objects
- Data Access Map
- DB Clients to Servers Map
- Active DB Users
- Cardholder DB Administration
- Source Programs
- Review Groups

PCI - Cardholder Server IPs    

Start Date: 2007-01-01 00:00:00 End Date: 2007-05-31 00:00:00

<u>Server IP</u>	<u>Server Type</u>	<u>Database Name</u>	<u>Count of Sessions</u>
192.168.1.186	ORACLE	CARD_DATA	8
192.168.2.51	ORACLE	CARD_DATA	140
192.168.200.108	DB2	CARD_DATA	182
192.168.200.108	DB2	DN8DEMO3	258
192.168.200.108	DB2	SAMPLE	44

Large WW financial institution addresses compliance

■ Challenge

- Address vulnerabilities in financial applications
- Needed enterprise-wide data security solution / fulfill emerging compliance requirements.
- Immediate focus on Sarbanes-Oxley Compliance (SOX) for critical financial application databases in both mainframe and distributed environments.
- Monitor privileged user activity, alerts on anomalies, generate audit reports to meet compliance

■ Solution

- Roll out of over 200 appliances of IBM InfoSphere Guardium (distributed and z/OS)

■ Benefits

- Support of compliance with SOX and other requirements.
- Proactively identified unauthorized or suspicious activities by continuously tracking all database actions – without impacting performance or modifying application databases.
- Detected / blocked unapproved activity by DBAs, developers and outsourced personnel without relying on native logs, triggers or other DBMS-resident mechanisms.
- Simplified audit with preconfigured reports and automated oversight workflows (electronic sign-offs, escalations, and so on).
- Ensure data governance by preventing unauthorized changes to critical database values or structures.
- BVA identified 5 year pay back period

European Bank

Improves delivery of reliable business applications & supported expanded international operations

Business challenge:

The bank wanted to implement a new testing methodology that focused on improving quality of its applications. Mainly industrializing the creation and management of testing environments, implementing a data masking solution and protecting sensitive data.

Solution:

IBM® provided the set of critical tools, Optim suite for the bank's data management team. It helps the bank migrate data from other systems and to mask data for testing. The main capabilities of the suite is to right-size test databases, refreshing and maintenance of production-like test environments and implementation of pre-defined masking techniques to support privacy regulations. The bank's implementation of IBM Optim automated the process of creating subsets of data for several accounts in minutes rather than hours.

Benefits:

- It enabled the bank to deliver reliable business applications and support its expanding retail, banking and insurance operations across international boundaries.
- It helped optimization of storage requirements, with small but realistic subsets, and the development of off-shoring activities with appropriate data masking.

Solution components:

- Information Management: Optim Data Masking Solution, Optim Data Masking Solution (z/OS)
- Optim Data Masking Solution for Siebel Customer Relationship Management
- Optim Test Data Management Solution, Optim Test Data Management Solution (z/OS)
- Optim Test Data Management Solution for Siebel Customer Relationship Management



Thank
YOU

The word "Thank" is written in a large, light blue, sans-serif font. Each letter contains a different portrait of a person. The "T" shows a man in a suit and orange tie. The "h" shows a woman with dark hair. The "a" shows a man with a green face. The "n" shows a man with a blue patterned shirt. The "k" shows a man with glasses. The word "YOU" is written in a similar font below "Thank". The "Y" shows a man looking at a laptop. The "O" shows a man in profile. The "U" shows a woman's profile.

Disclaimer/Trademarks

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements, or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

The information on the new products is intended to outline our general product direction and it should not be relied on in making a purchasing decision. The information on the new products is for informational purposes only and may not be incorporated into any contract. The information on the new products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. The development, release, and timing of any features or functionality described for our products remains at our sole discretion.

This information may contain examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious, and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Trademarks The following terms are trademarks or registered trademarks of other companies and have been used in at least one of the pages of the presentation:

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both: DB2 Universal Database, eServer, FlashCopy, IBM, IMS, iSeries, Security, z/OS, zSeries, Guardium, IBM Smart Analytics Optimizer, Data Encryption Tool for IMS and DB2 Databases, DB2 Administration Tool / DB2 Object Compare for z/OS, DB2 Audit Management Expert for z/OS, DB2 Automation Tool for z/OS, DB2 Bind Manager for z/OS, DB2 Change Accumulation Tool for z/OS, DB2 Cloning Tool for z/OS, DB2 High Performance Unload for z/OS, DB2 Log Analysis Tool for z/OS, DB2 Object Restore for z/OS, DB2 Path Checker for z/OS, DB2 Query Management Facility for z/OS, DB2 Query Monitor for z/OS, DB2 Recovery Expert for z/OS, DB2 SQL Performance Analyzer for z/OS, DB2 Table Editor for z/OS, DB2 Utilities Enhancement Tool for z/OS, DB2 Utilities Suite for z/OS, InfoSphere Change Data Capture, InfoSphere Data Event Publisher, InfoSphere Replication Server, Optim Data Growth Solution for z/OS, Optim Development Studio, Optim pureQuery Runtime, Optim Query Workload Tuner, Optim Test Data Management Solution for z/OS, Security OMEGAMON XE for DB2 Performance Expert on z/OS

EMC and TimeFinder are trademarks of EMC Corporation

Hitachi is a trademark of Hitachi Ltd

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.