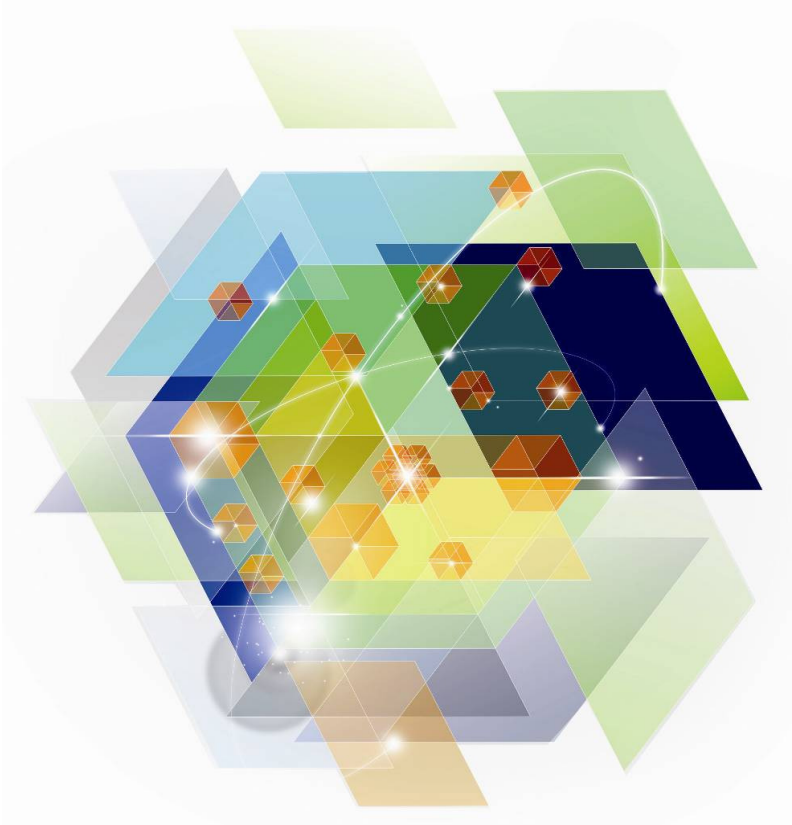
IMS Data Governance

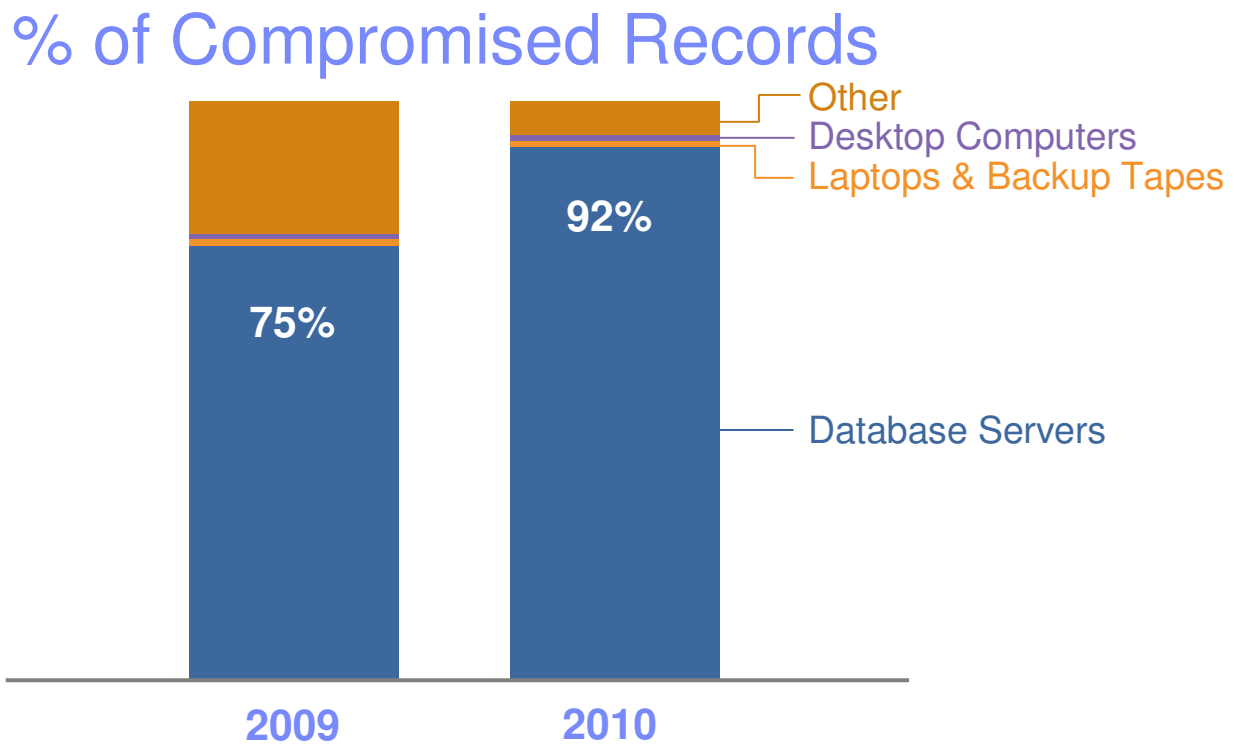
Claudine Bouloc

Certified L2 Client Technical Professional
Information Management
IBM Software Group



© 2012 IBM Corporation

Database servers are the primary source of breached data



Sources: Verizon Business Data Breach Investigations Report 2009, 2010

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.

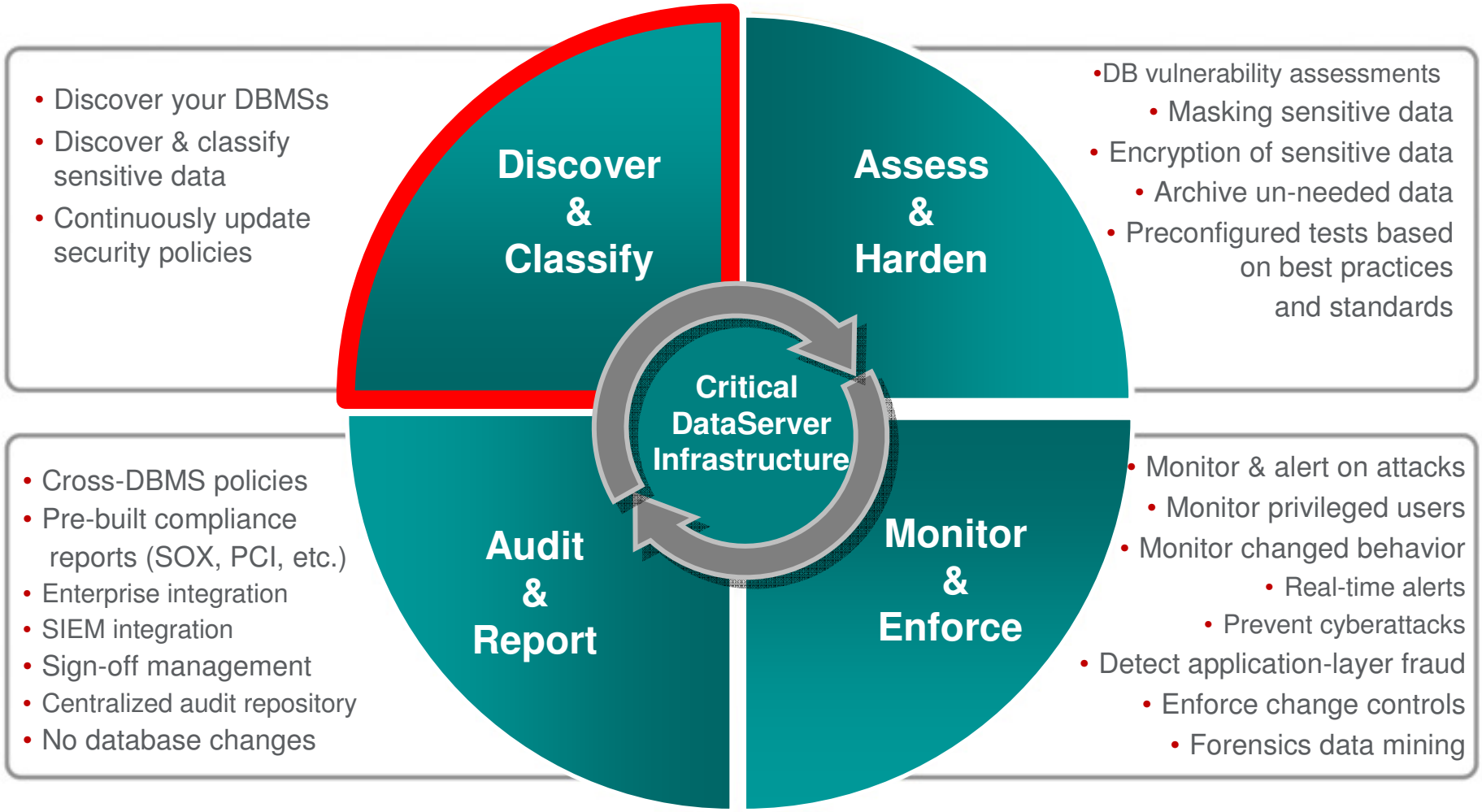
© 2012 IBM Corporation

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.

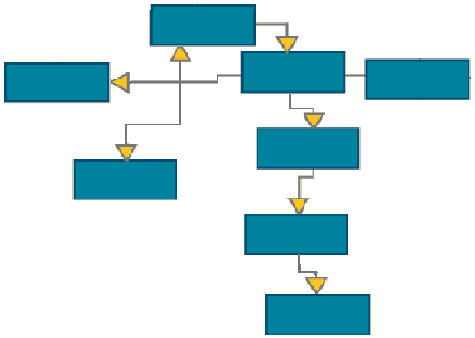
© 2012 IBM Corporation

Address the Full Data Protection Lifecycle



© 2012 IBM Corporation

Understanding a Complete Business Object



Represents application data record – payment, invoice, customer

- Referentially-intact subset of data across related tables and applications; includes metadata

Provides “historical reference snapshot” of business activity

Federated extract support across enterprise data stores

© 2012 IBM Corporation

Sensitive Data Discovery

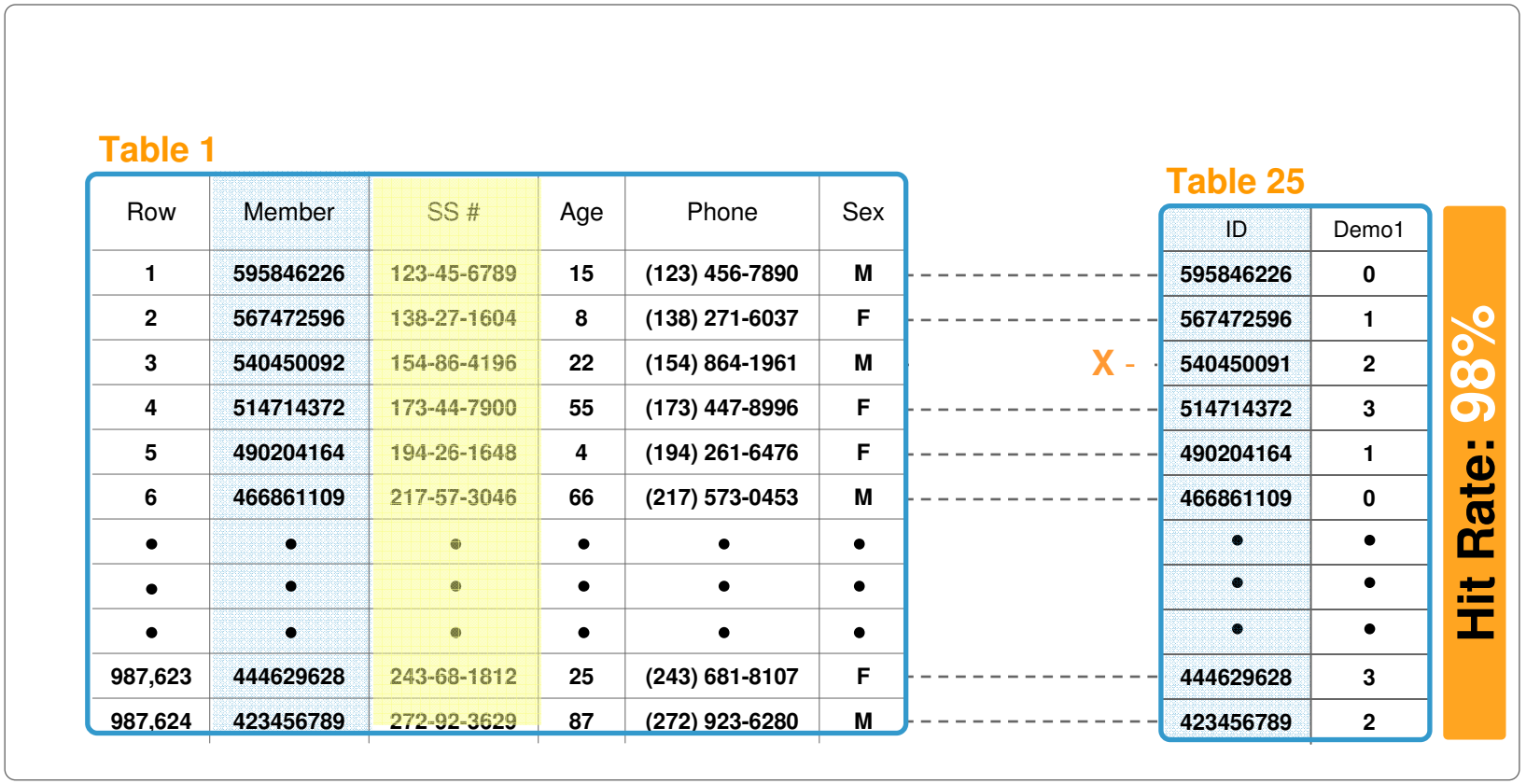
- **Common PII data element discovery**
  - Pre-Defined Scanning
- **Custom sensitive data discovery**
  - Supply Discovery with “descriptions/examples”
    - *Patterns*
    - *Data examples*.
  - Discovery will scan for matching columns
- **Hidden sensitive data discovery**
  - Sensitive data embedded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

© 2012 IBM Corporation

InfoSphere Discovery Speeds Understanding Data

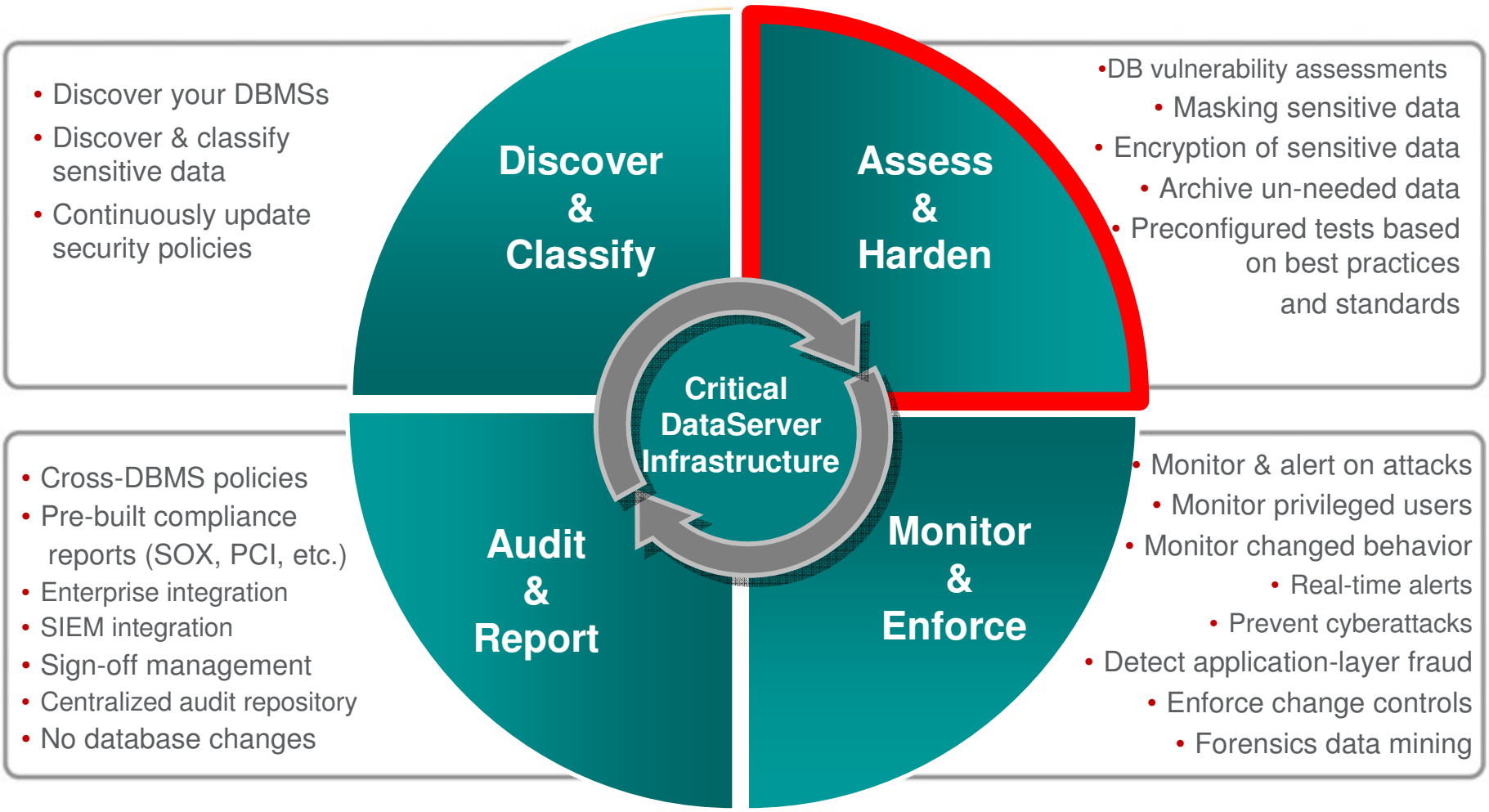
IBM InfoSphere Discovery

The Discovery Engine analyzes **data values** to **automatically discover** the columns that **relate rows** across data sources, and the columns which contain **sensitive data**.



© 2012 IBM Corporation

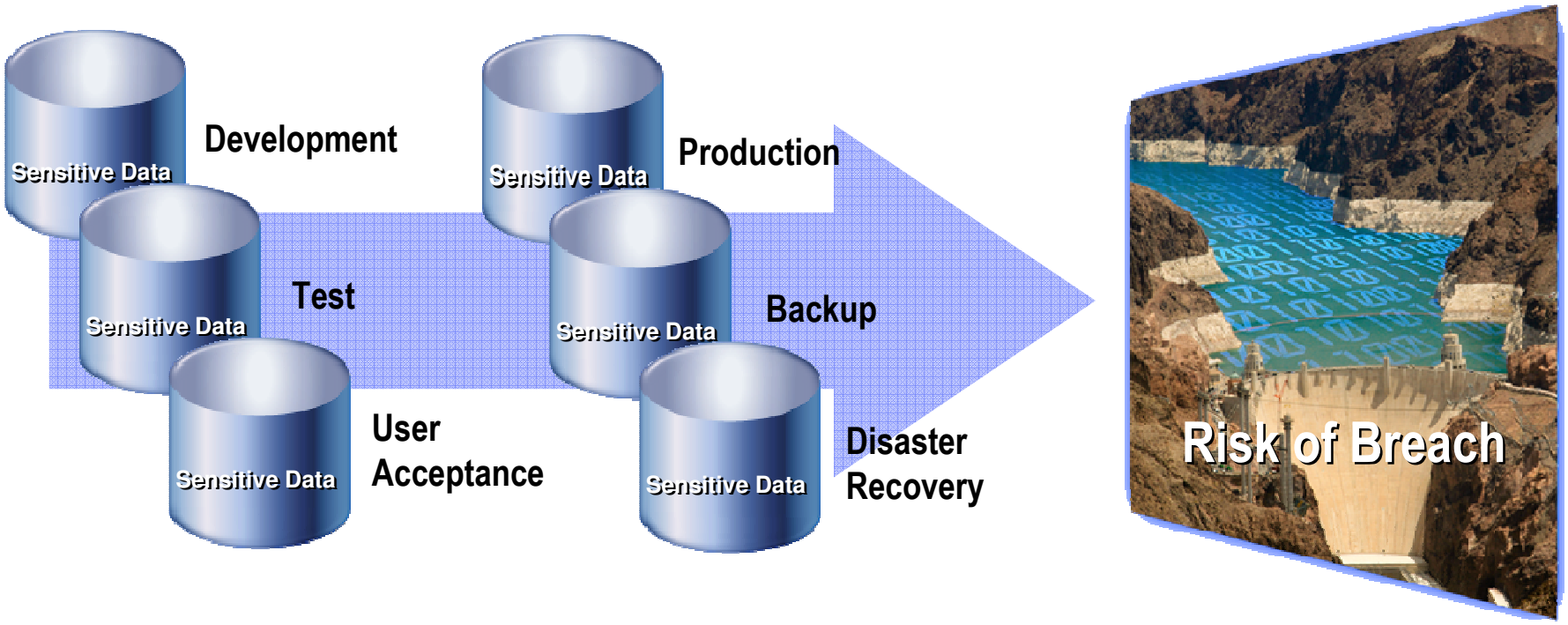
Address the Full Data Protection Lifecycle



© 2012 IBM Corporation

Limit the scope of compliance and security concerns

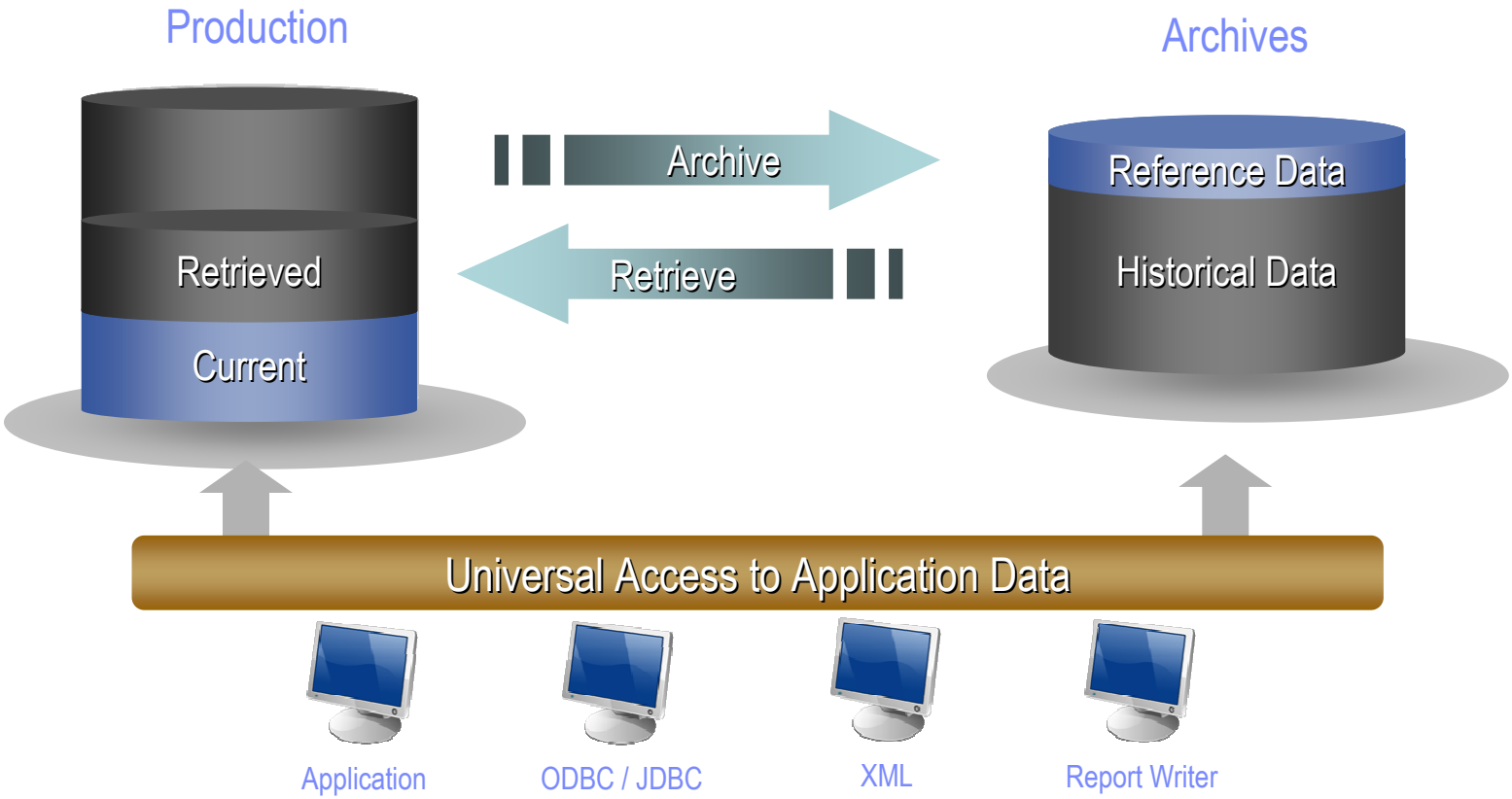
Sensitive Data Proliferation



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

© 2012 IBM Corporation

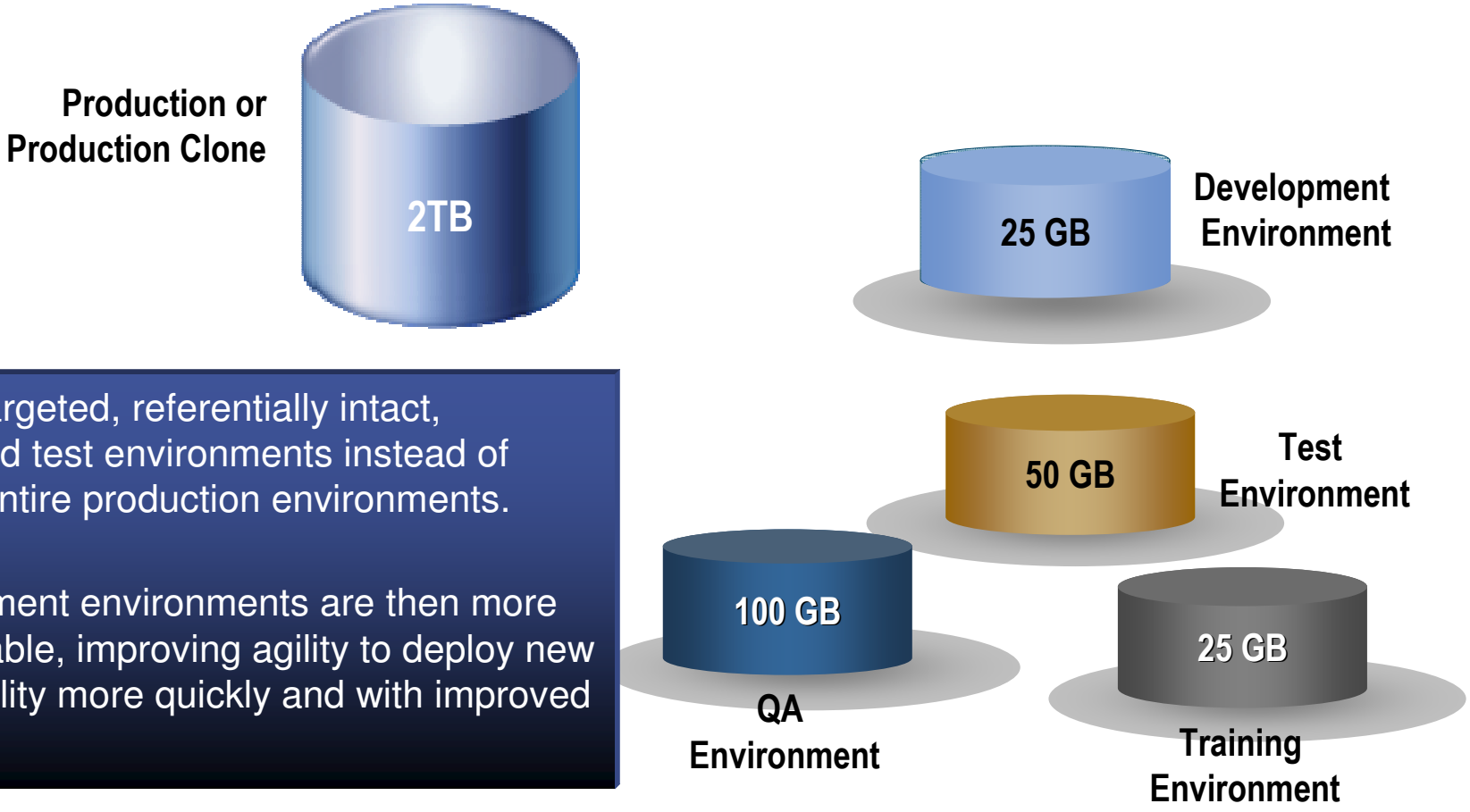
Archive inactive data to limit compliance scope



Archiving is an intelligent process for *moving* inactive or infrequently accessed data that still has *value*, while providing the ability to *search and retrieve* the data

© 2012 IBM Corporation

Effective Test Data Management



Create targeted, referentially intact, right-sized test environments instead of cloning entire production environments.

Development environments are then more manageable, improving agility to deploy new functionality more quickly and with improved quality.

Out-of-the-box subset support for packaged ERP/CRM applications:

ORACLE e-businesssuite | PeopleSoft | SIEBEL | JDEdwards Enterprise Software | SAP | Other

© 2012 IBM Corporation

Sensitive Data Masking

Masked or transformed data must be appropriate to the context:

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

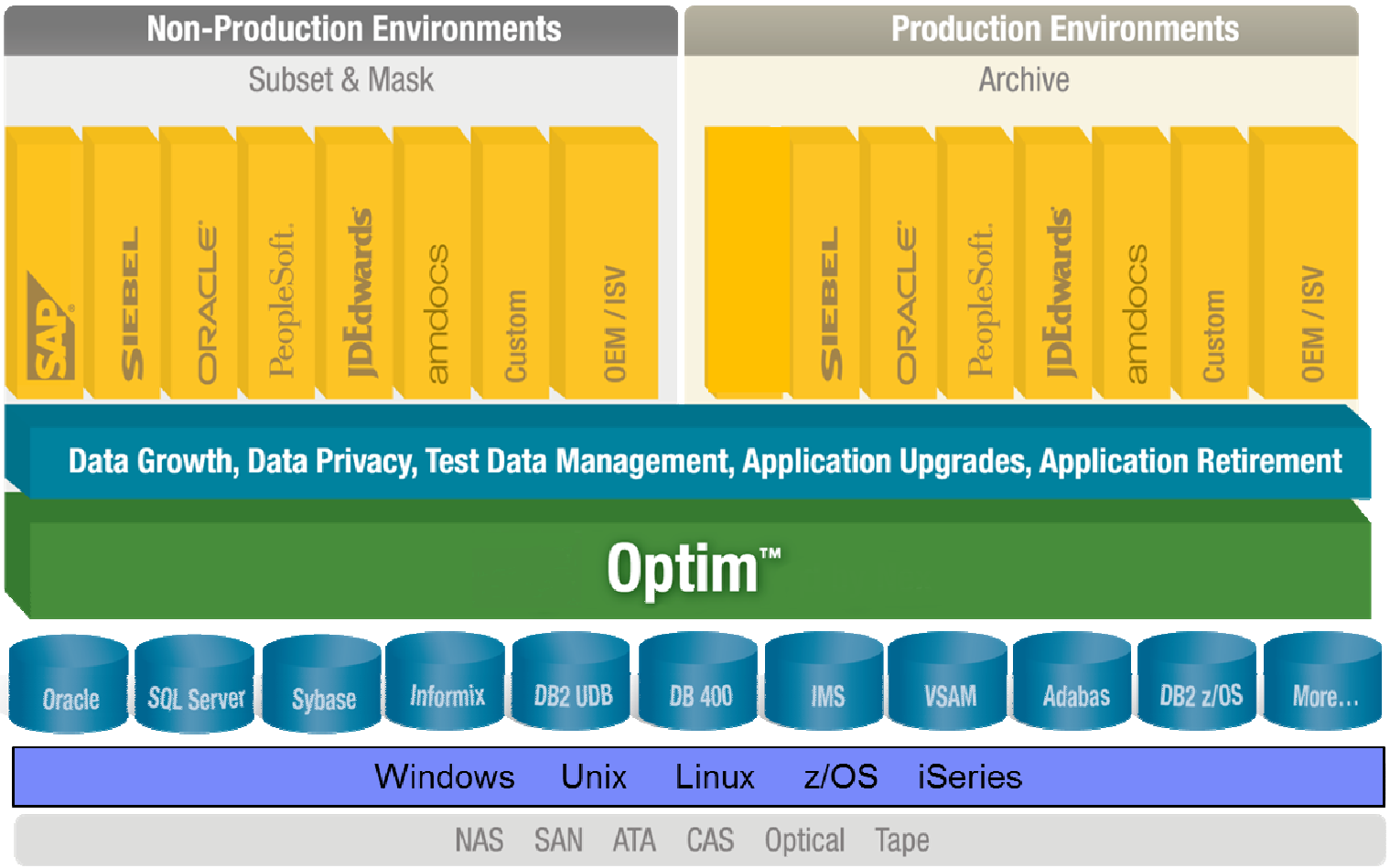
Event Table

PersNbr	FstNEvtOwn	LstNEvtOwn
10002	**Pablo**	**Picasso**
10002	**Pablo**	**Picasso**

© 2012 IBM Corporation

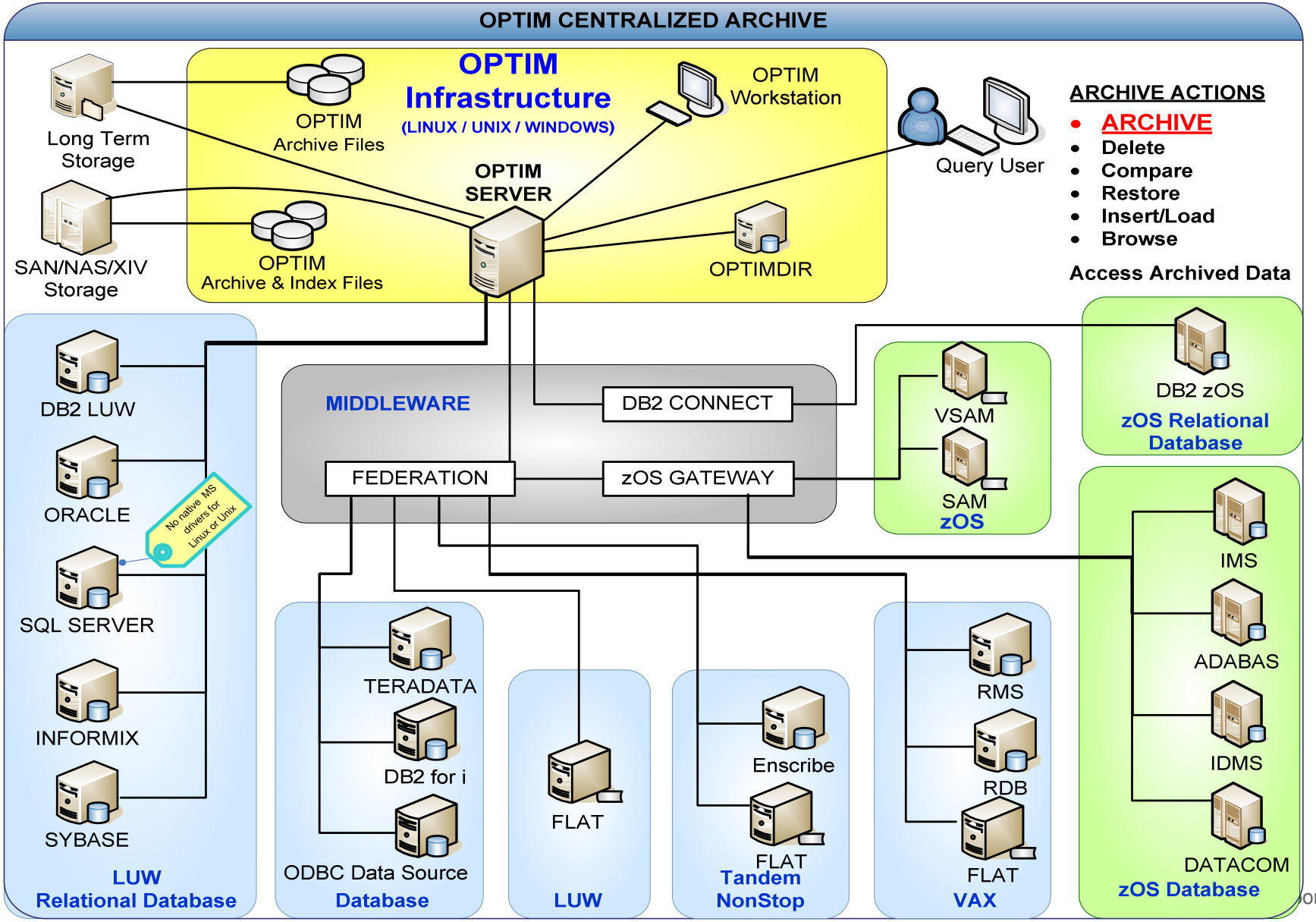
Optim's Enterprise Architecture

- Single scalable architecture provides central point to extract, store, restore, and protect (mask) application data records

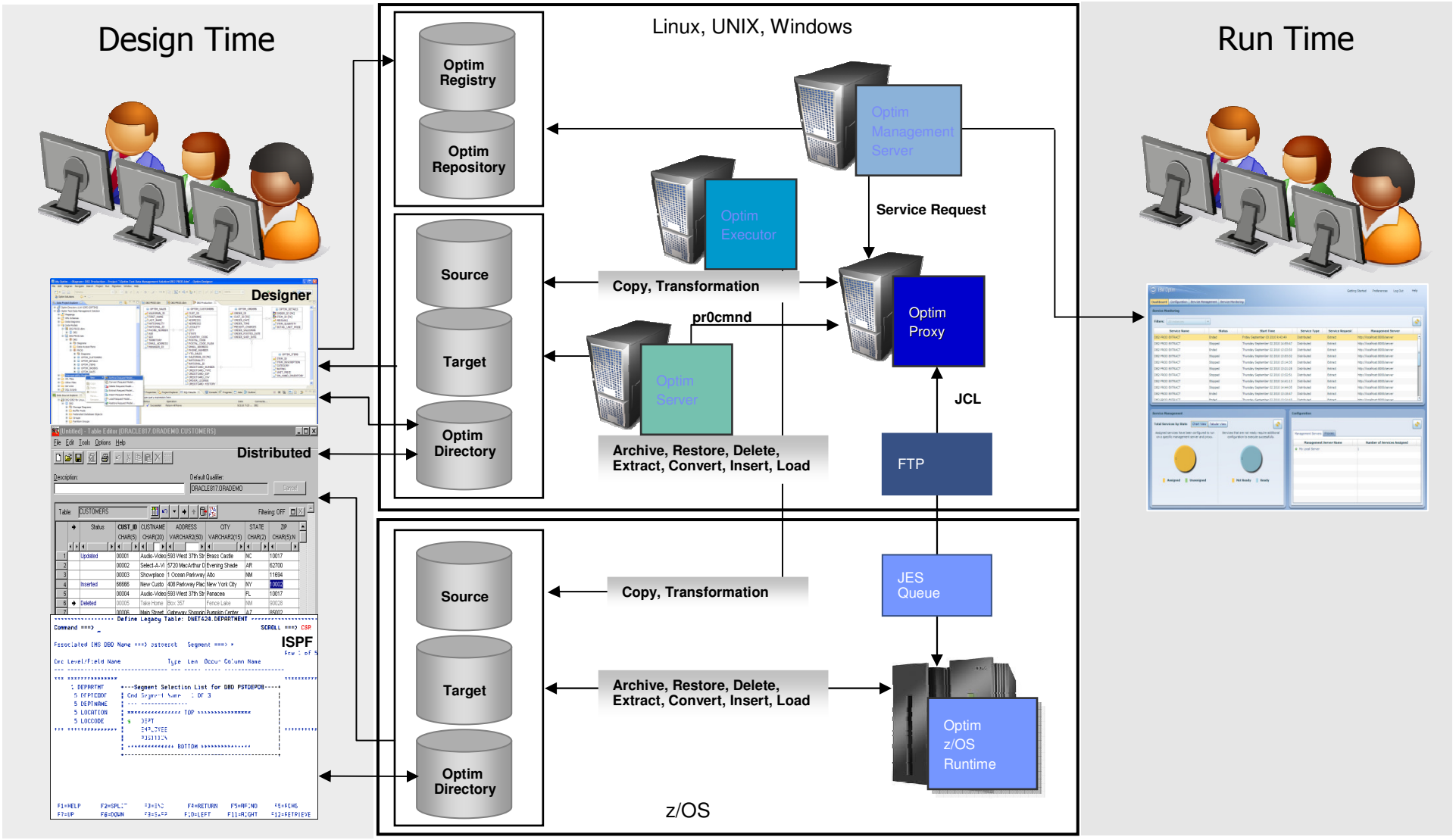


© 2012 IBM Corporation

Infosphere Optim centralized architecture



Optim Architecture: Designer and Manager



© 2012 IBM Corporation

OPTIM for z/OS Family of Product

- **Test data management (TDM)**
  - Approach to creating and managing test or non-production environments to meet the needs of various stakeholders and business requirements.
    - Extract related subsets of production data that are targeted to functionality under test
    - Quickly and easily refresh test environments
  - Improvement for application quality & customer satisfaction
  - Support for DB2, IMS DB, VSAM
- **Data Masking (DM)**
  - Removing, masking or transforming elements that could be used to identify an individual
    - De-identify data for privacy protection
    - Compare “before” and “after” images of test data
  - Support for DB2, IMS DB, VSAM
- **Database archiving and application’s data retirement with Data Growth (DG)**
  - Segregate historical data to secure archive
  - Align performance to service level targets
  - Reclaim underutilized capacity
  - Support for DB2, IMS DB, VSAM
    - IMS DB and VSAM support provided by Distributed Data growth based on Classic Federation on z/OS and InfoSphere Federation Server

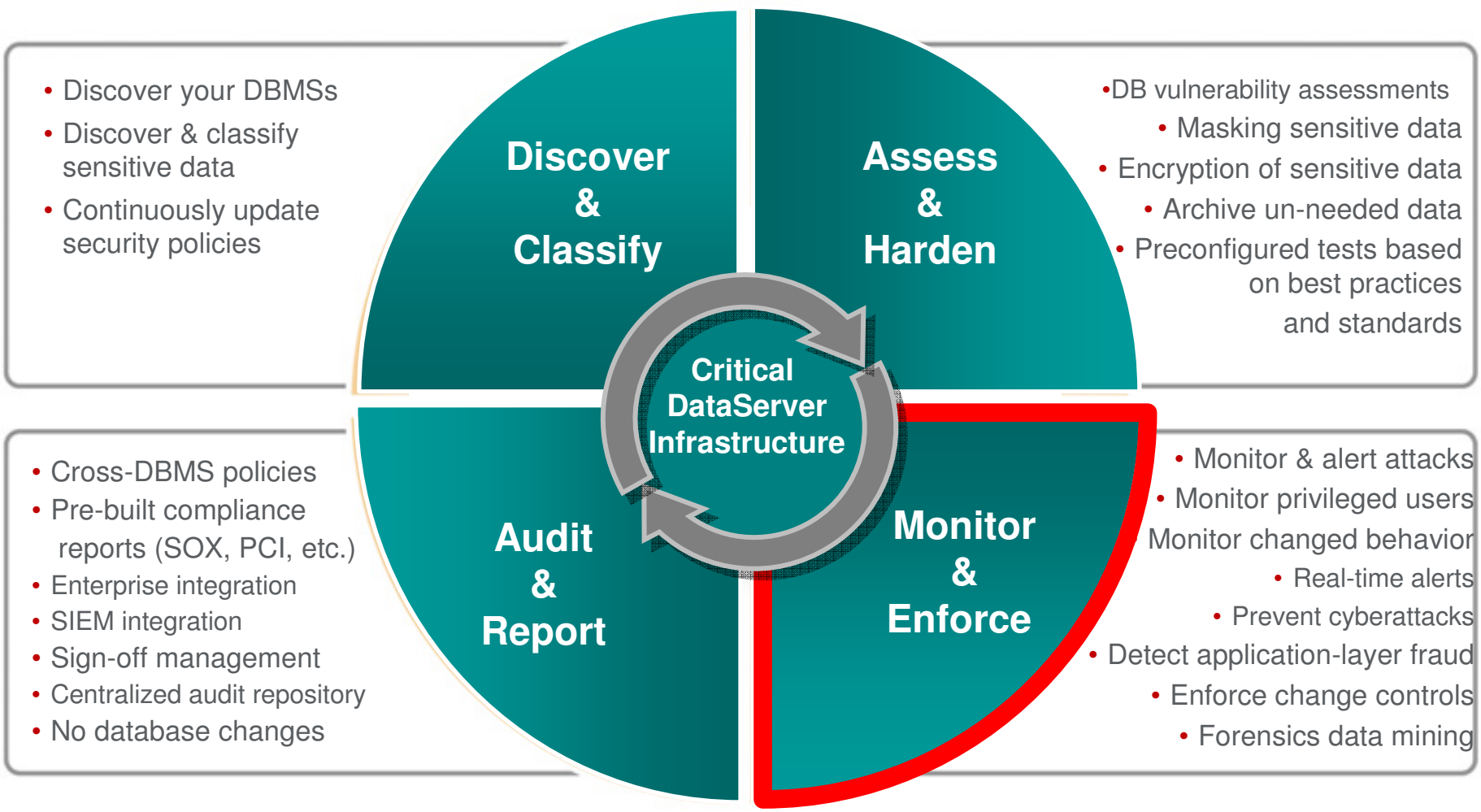
© 2012 IBM Corporation

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

© 2012 IBM Corporation

Address the Full Data Protection Lifecycle



© 2012 IBM Corporation

Customer Challenges: Auditing on z/OS

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

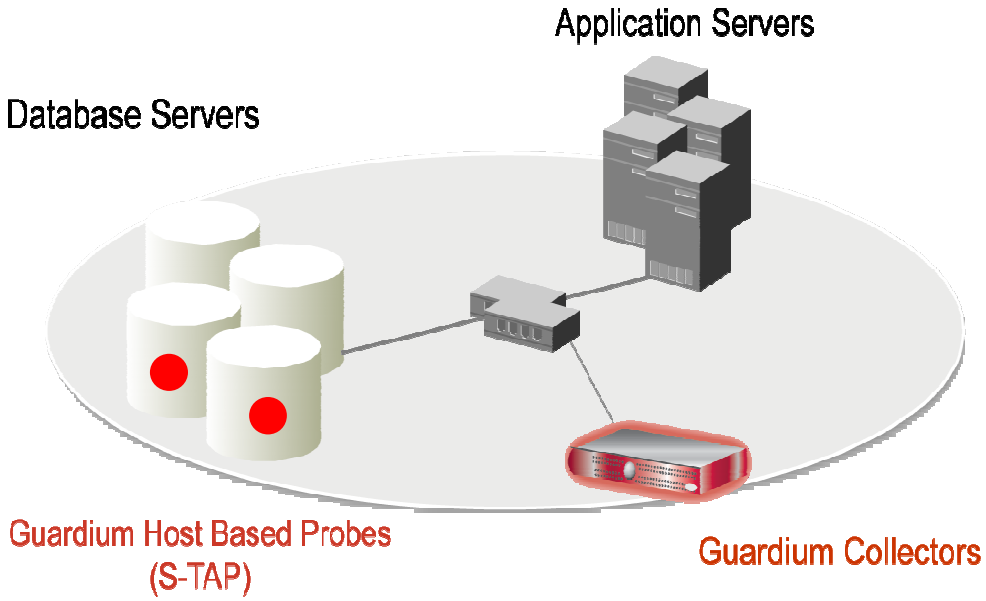
© 2012 IBM Corporation

Guardium for z

- **Provides a single unified view and secure audit trail of all database activities – across *both* mainframe and distributed environments**
  - Enterprise-wide compliance reporting, analytics & forensics
- **Can be managed by non-DBAs, thereby supporting SoD**
- **Reduces compliance cost and effort via automated and centralized controls (vs. manual, ad hoc processes)**
  - With compliance workflow automation (sign-offs, escalations, …)
- **Based on mainframe technology developed by IBM**
- **Minimal impact on performance**

© 2012 IBM Corporation

Guardium Database Activity Monitoring



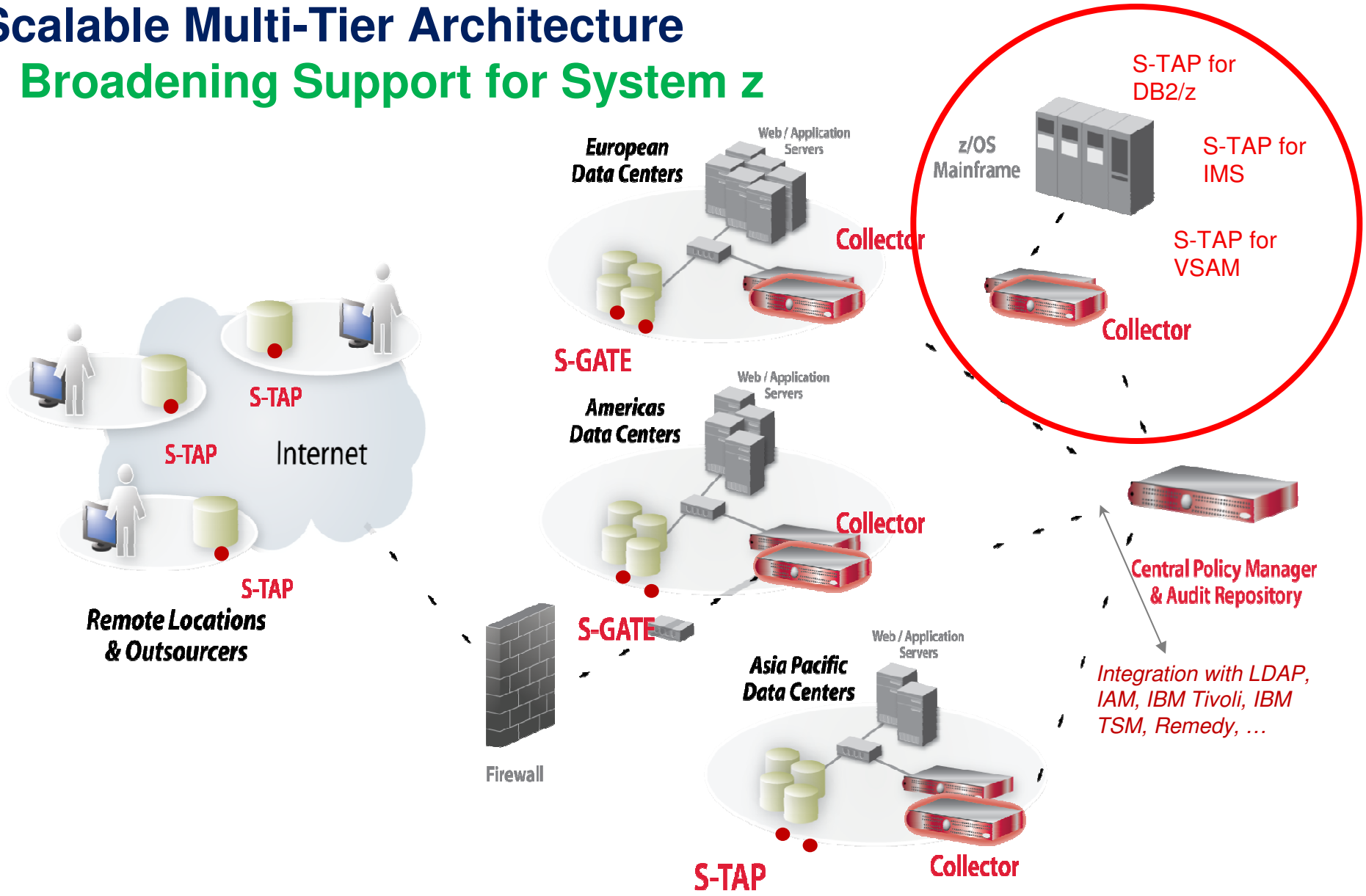
- Non-invasive architecture
  - Outside database
  - Minimal performance impact
  - No DBMS or application changes
- Cross-DBMS solution
- 100% visibility including local DBA access

- 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.)

© 2012 IBM Corporation

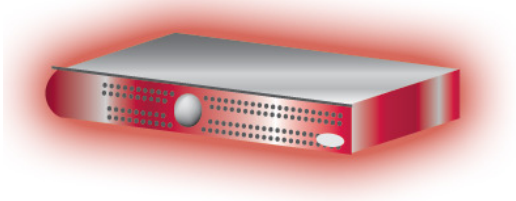
Scalable Multi-Tier Architecture

Broadening Support for System z



© 2012 IBM Corporation

InfoSphere Guardium Appliance



- **The Appliance is a stand alone box**
  - Hardened Linux OS and DBMS kernel
  - Pre-configured, firmware updated
  - Secure audit repository
    - All audit information is stored in a secure repository that cannot be modified by anyone—even privileged users
- **Root access to the appliance is not provided**
  - Prevents administrators from accessing the base OS, file system, or embedded database to view or modify audit data
- **Appliance collects audit data from different agent 'probes‘ like S-TAP**
- **End user access is via Web Browser application**

© 2012 IBM Corporation

Guardium for System z Version 8.2

- New support for IMS
  - New S-TAP for IMS
  - Capture IMS activity for delivery to Guardium Appliance
  - Real-Time monitoring of IMS events
  - Comprehensive Auditing of IMS
  - Custom IMS security and compliance reports

- New support for VSAM
  - New S-TAP for VSAM
  - Capture VSAM file activity to enhance your DB monitoring
  - VSAM security and compliance reporting

- Enhanced support for DB2/z
  - Ongoing performance improvements
  - Unified administration of DB2 S-TAP within the Guardium appliance
  - Elimination of FTP – all event data is streamed in real-time
  - Increased filtering flexibility of authorization id's

- Enhanced support for DB2/z Vulnerability Assessment

© 2012 IBM Corporation

Guardium S-TAP for IMS Collection Overview

Databases

- All Reads of IMS DBs and segments using IMS DLI GET calls (GN, GU, GNP, etc).
- Changes, INSERT, UPDATE and DELETE calls (REPL, ISRT, DLET)
- Same for IMS Batch jobs and IMS Online regions

Segments

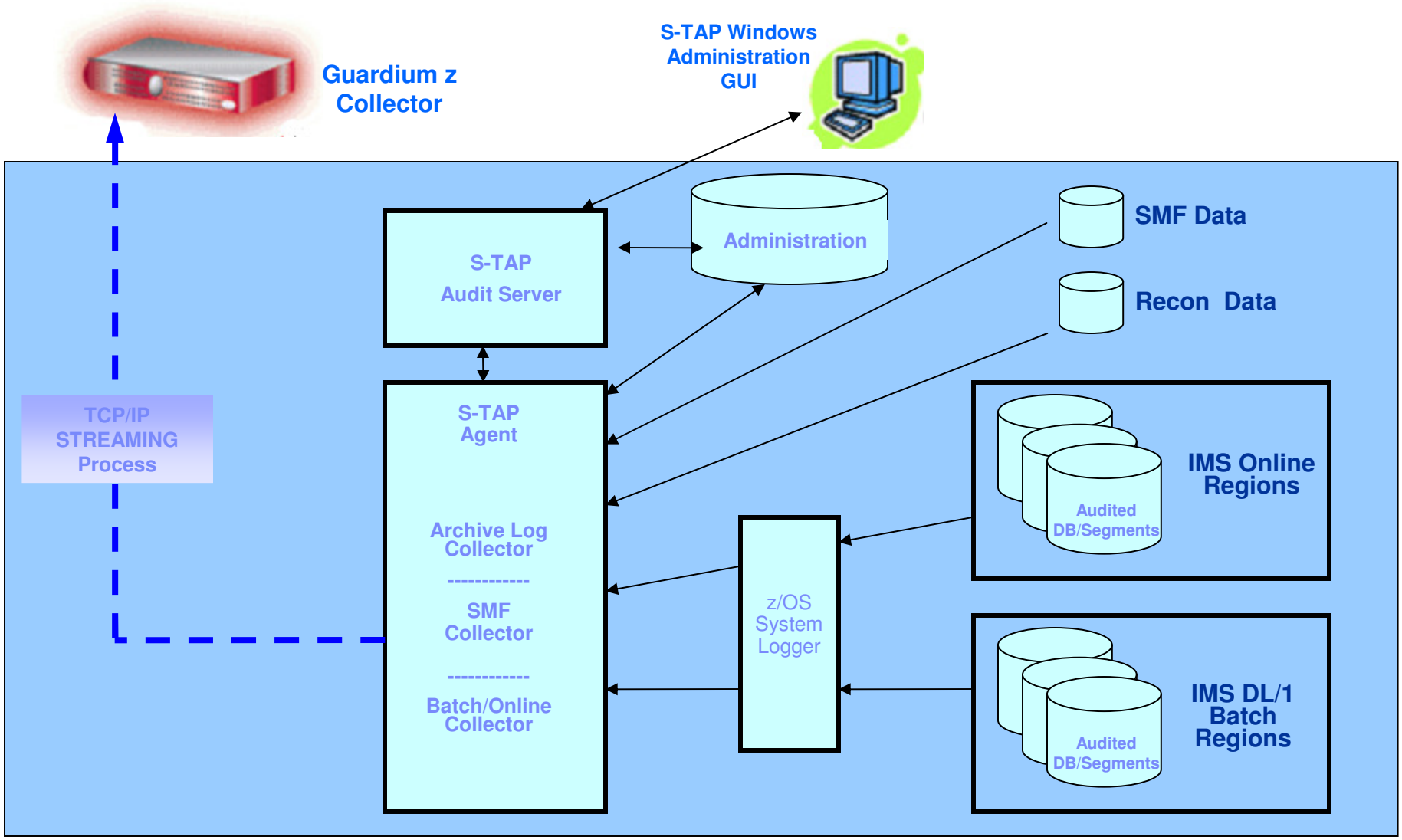
- Ability to audit and report READ, INSERT, UPDATE, and DELETE calls on specific database segments
- READ and DELETE calls retain the concatenated key of the audited segment
- UPDATE and INSERT calls retain the concatenated key of the audited segment as well as the segment data, as found in the DLI call I/O area

You can select which calls to audit per target

- For example: all databases, all segments, one DB and one segment of the DB,
- each segment can have different calls audited
- When a call is to be collected, the relevant information is gathered
  - e.g. call type, userid, PSB name, DBName, Segment Name, etc.
  - We do not gather the segment search argument

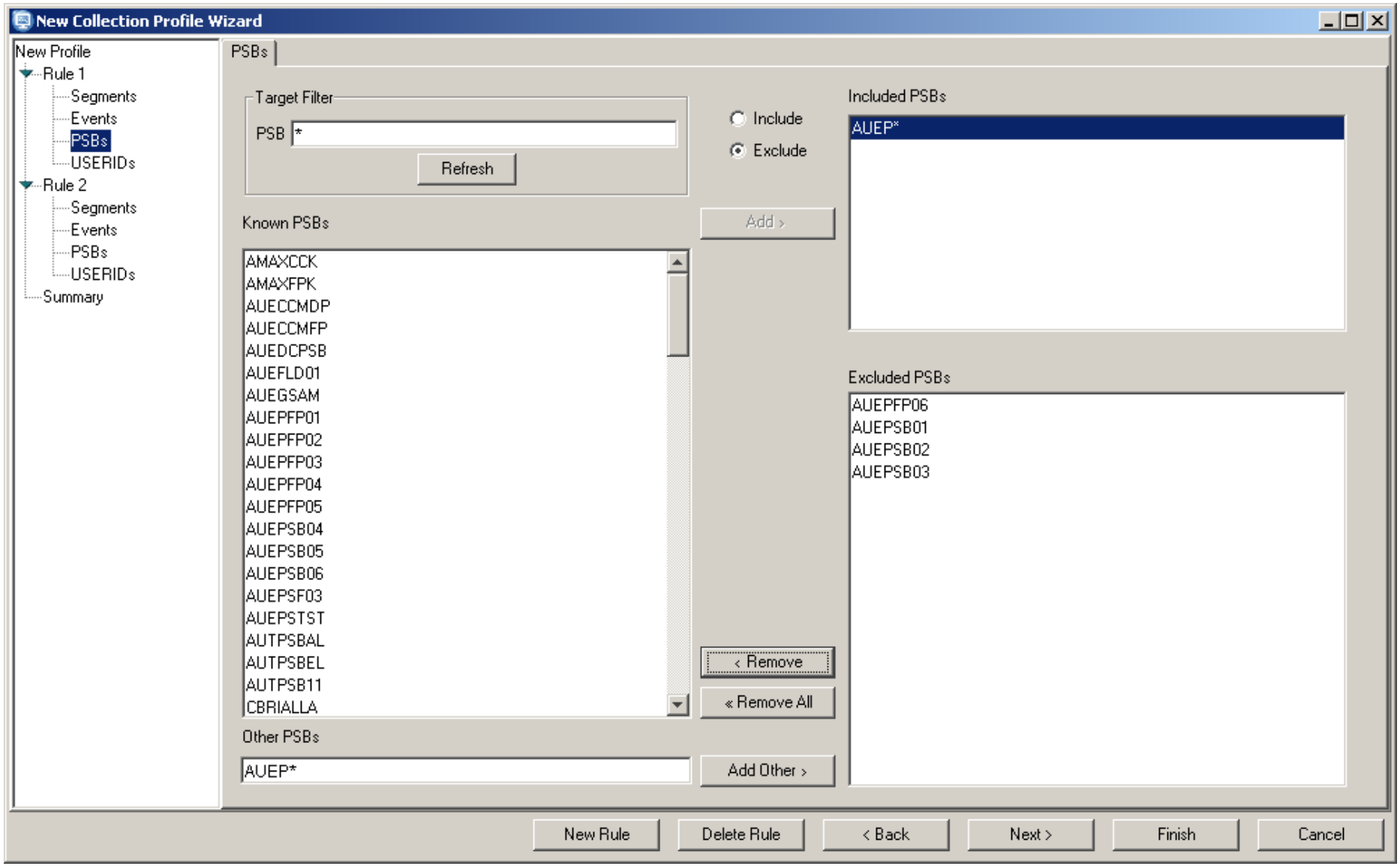
© 2012 IBM Corporation

Guardium S-TAP for IMS on z/OS Architecture



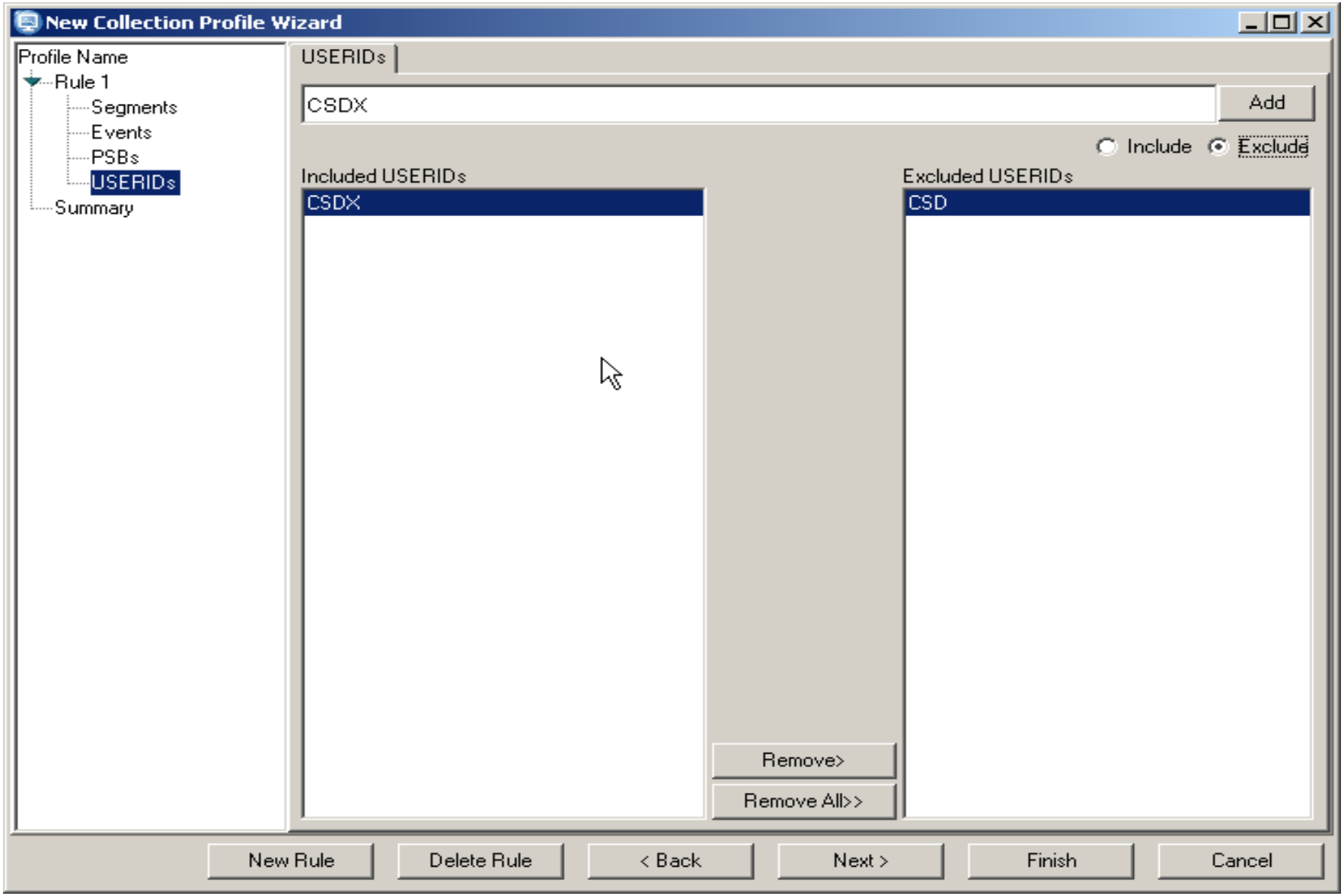
© 2012 IBM Corporation

PSB Collection



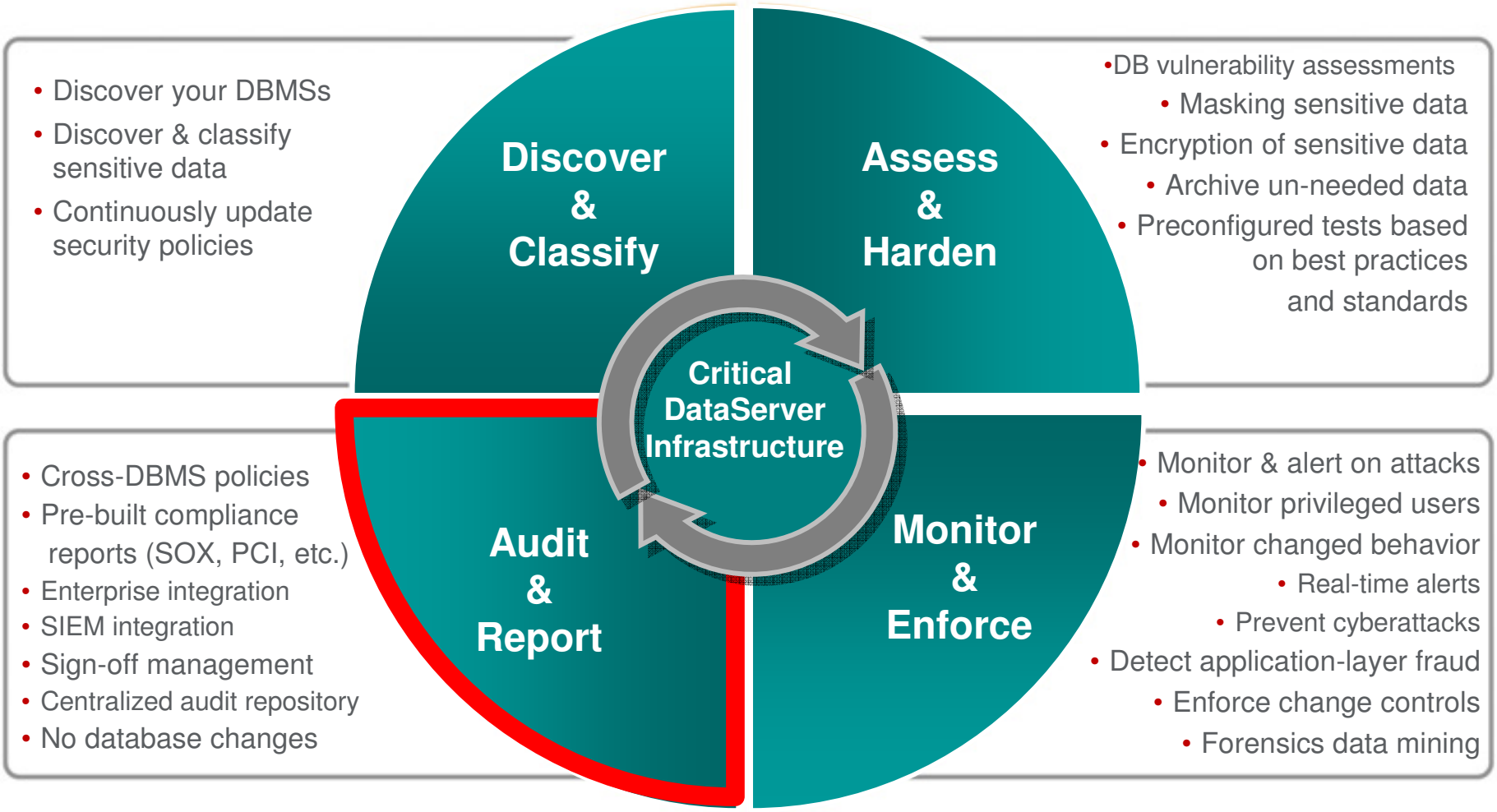
© 2012 IBM Corporation

USERID Collection



© 2012 IBM Corporation

Address the Full Data Protection Lifecycle



© 2012 IBM Corporation

IMS Data integrated into Guardium reporting

IMS DLI Summary 2

Start Date:	2011-08-10 06:00:00	End Date:	2011-08-10 08:00:00
Aliases:	OFF	Database:	LIKE %
IMS_Name:	LIKE %12	JobName:	LIKE %
JobNumber:	LIKE %	PSB_Name:	LIKE %
Segment:	LIKE %	UserID:	LIKE %

Min Timestamp	Max Timestamp	IMS Context	IMS Job Name	IMS Job Number	IMS Database	IMS Segment	IMS User ID	IMS PSB Name	Servic Name
2011-08-10 06:11:02.0	2011-08-10 06:11:02.0	DB Level GET	TSTCMDDC	J0053357	AUECCMDD	LEVELF	CSIVANA	AUECCMDP	IMSV1:
2011-08-10 06:11:02.0	2011-08-10 06:11:02.0	DB Level REPLACE	TSTCMDDC	J0053357	AUECCMDD	LEVELF	CSIVANA	AUECCMDP	IMSV1:
2011-08-10 06:11:02.0	2011-08-10 06:11:02.0	Segment Level GET	TSTCMDDC	J0053357	AUECCMDD	LEVEL5	CSIVANA	AUECCMDP	IMSV1:
2011-08-10 06:11:02.0	2011-08-10 06:11:02.0	Segment Level GET	TSTCMDDC	J0053357	AUECCMDD	LEVELC	CSIVANA	AUECCMDP	IMSV1:
2011-08-10 06:11:02.0	2011-08-10 06:11:02.0	Segment Level REPLACE	TSTCMDDC	J0053357	AUECCMDD	LEVEL5	CSIVANA	AUECCMDP	IMSV1:
2011-08-10 06:11:02.0	2011-08-10 06:11:02.0	Segment Level REPLACE	TSTCMDDC	J0053357	AUECCMDD	LEVELC	CSIVANA	AUECCMDP	IMSV1:
2011-08-10 06:11:07.0	2011-08-10 06:11:07.0	DB Level GET	TSTCMDFC	J0053358	AUECCMFD	LEVELF	CSIVANA	AUECCMFP	IMSV1:
2011-08-10 06:11:07.0	2011-08-10 06:11:07.0	DB Level REPLACE	TSTCMDFC	J0053358	AUECCMFD	LEVELF	CSIVANA	AUECCMFP	IMSV1:
2011-08-10 06:11:07.0	2011-08-10 06:11:07.0	Segment Level GET	TSTCMDFC	J0053358	AUECCMFD	LEVEL5	CSIVANA	AUECCMFP	IMSV1:

© 2012 IBM Corporation

© 2012 IBM Corporation

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, Tivoli, 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, Tivoli OMEGAMON XE for DB2 Performance Expert on z/OS
EMC and TimeFinder are trademarks of EMC Corporation
Hitachi is a traademark of Hitchi 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.

© 2012 IBM Corporation