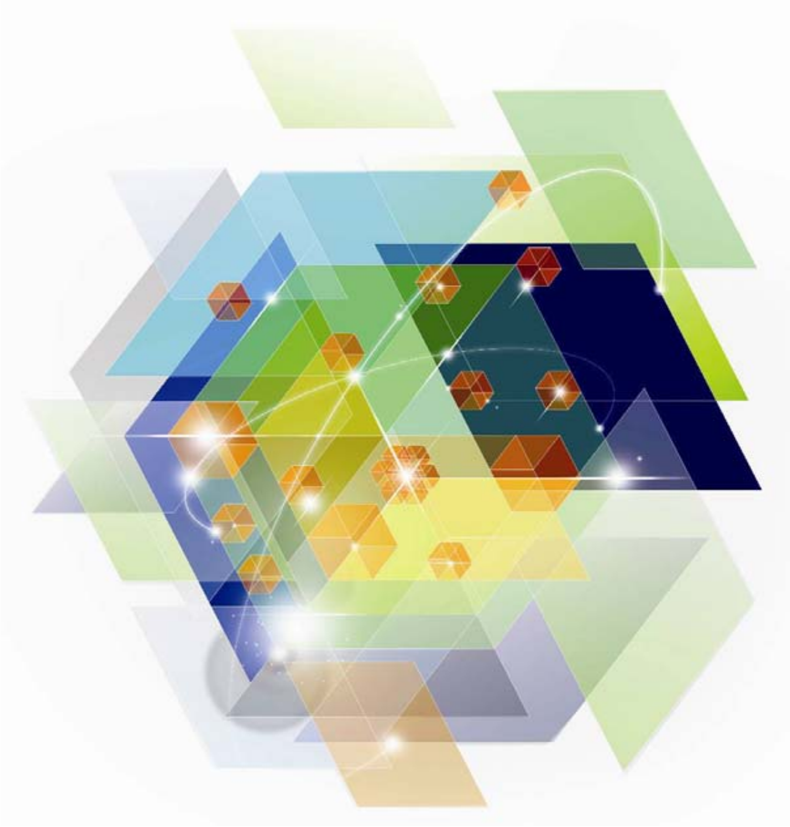
IBM System z Technology Summit

Protecting the Database Environment on z/OS

Presenter Name

Title



What we will discuss

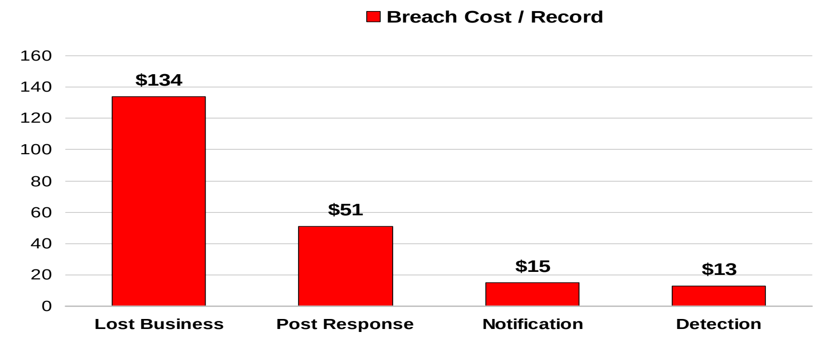
- **DB2 10 Security Enhancements**
  - New ways to protect your data from ad hoc applications
  - Allow DB2 to automatically mask or filter data returned to all applications
  - Allow administrators to do their job without exposing sensitive business data
  - New feature to audit privileged users and all SQL access
- **Data Lifecycle Management, Test Data Generation, and Obfuscation**
- **Database Activity Monitoring and Real-time Protection**
- **Data-at-Rest Encryption**
- **Resources**
  - DB2 publications is a good source of information to help migrate to the new features
  - New DB2 10 Security Redbook and Redpaper to help understand the new features
- **Q&A and Summary**

Cost of a Data Breach
Understand What's at Stake – Top 5 Breaches by Cost

Rank	Company	Records Breached	Estimated Cost
1	Major consumer retailer	100 Million Records	$2 Billion
2	Multichannel Marketer	150 Million Records	$225 Million to $4 Billion
3	Major consumer retailer	45 Million Records	$256 Million
4	Credit card payment processor	100 Million Records	$140 Million
5	US Government Agency	17 Million Records	$30 Million

Total Cost of Breached Record 2011: $214

Cost / Breached Record Breakdown



Mainframe Breach

xxx: At least 45.7 million credit and debit card numbers were stolen by hackers who accessed the Mainframe computer systems at the xxx. The cost of **breach Financial Impact:** $256 Million Remediation (2007)

DB2 Security Challenges

- **Need ways to protect data from both your database administrators as well as your database applications**
  - New ways to meet auditor demands
  - Control administrators access to data
  - Little control of privileged IDs
  - Little or no individual accountability
  - Difficult to manage or audit data
  - Little control of implicit privileges
  - No migration path

Recent Banking Business Value Assessment Executive Summary

Current State Assessment & Top Challenges

The current mainframe monitoring processes are custom-built created by the same people it is meant to monitor. Reporting is run nightly resulting in a non-trivial window for an exposure to occur. Most importantly, the SYSADM ID represents an audit blind spot as activity under this ID cannot by fully monitored. If this blind spot is left unchecked, it leaves a vulnerability that could result in a significant data breach

- No real-time processes with limited audit data forensics
- No rules based behavioral & correlation of DB activities
- No confidential data identification and/or monitoring
- Insufficient separation of duties (SOD)
- Insufficient super ID monitoring

z/OS built-in security provides a firewall around DB2

SAF protects all user access to DB2
Optionally protect all data access

z/OS authenticates all users and prevents unauthorized access from specific security network zones

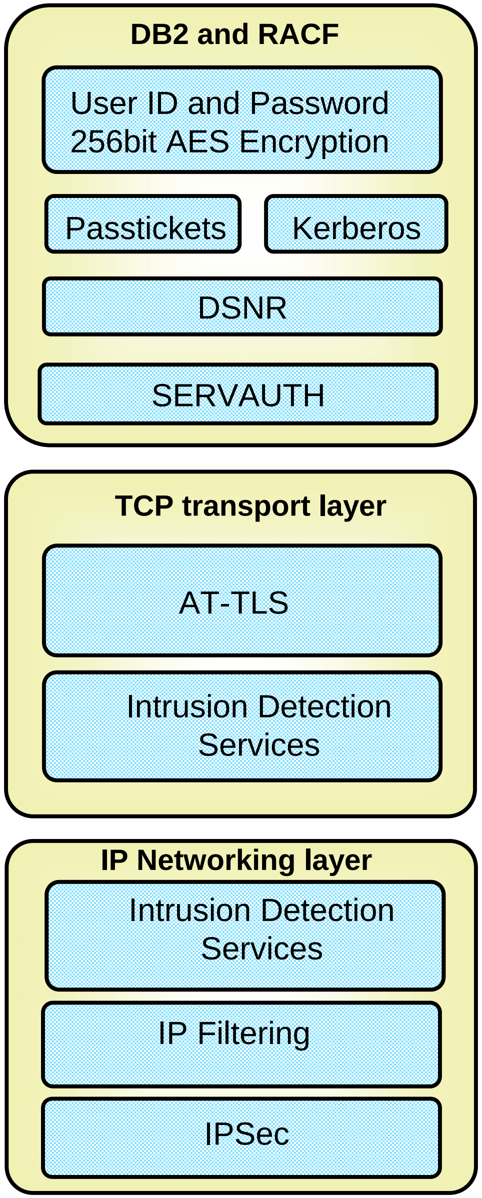
Communications Server creates a protective zone around DB2

Application Transparent -TLS is transparent to DB2
*Certificate Authentication

IDS protection is provided in two layers

IP packet filtering blocks out all IP traffic that the DB2 server doesn't specifically permit.

IPSec is transparent to upper-layer protocols



DB2 and RACF

User ID and Password
256bit AES Encryption

Passtickets

Kerberos

DSNR

SERVAUTH

TCP transport layer

AT-TLS

Intrusion Detection Services

IP Networking layer

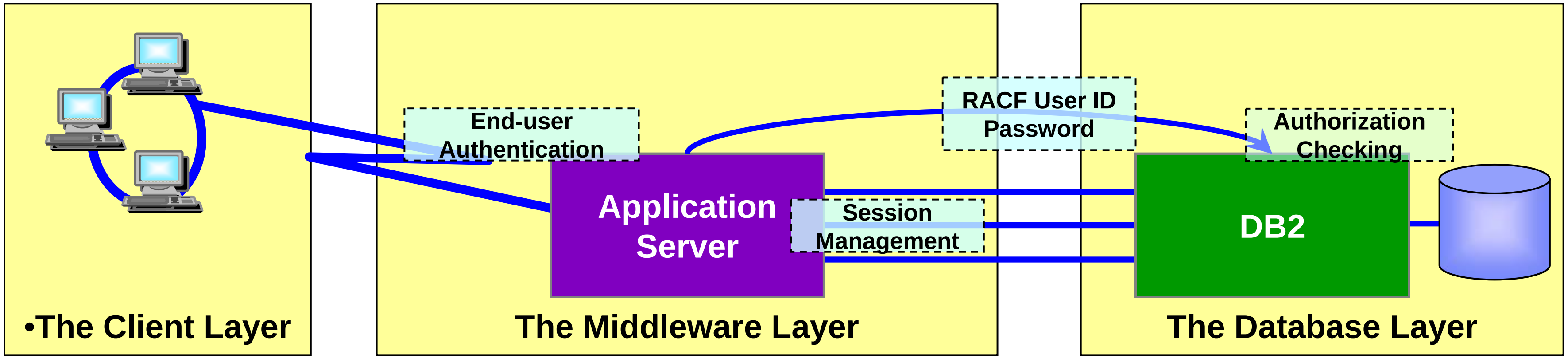
Intrusion Detection Services

IP Filtering

IPSec

DB2 Security Challenges

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

Better Protection and Auditing capability built-into DB2 10

- Improved Data Protection
  - Minimize the need for superuser 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

Database Tasks
Security Tasks
System Tasks
Temporal Data
SQL Auditing
Row & Column Access Controls

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

New 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 r

Migration path to exploit new authorities

New SEPARATE_SECURITY installation parameter

Reduces the capabilities of SYSADM and SYSCTRL to better exploit the new system DBADM authorities

- SYSADM and SYSCTRL can no longer grant or revoke privileges
- SYSADM can not longer SET SQLID to any user
- SYSADM should be used to perform system tasks only

Control cascading effect of revokes: REVOKE_DEP_PRIVILEGES

- Migration path to new the new system DBADM authorities
- New revoke dependent privileges install parameter
- New revoke dependent privileges SQL clause

New audit policies capability provide needed flexibility and functionality

- New audit policies managed in catalog
- Audit privileged users
- Audit SQL activity against a table
- Audit distributed identities

- **New auditing capability allows you to collect auditing data using DB2 native trace capabilities**

New Audit Policies Feature

- **Auditor can audit all SQL access using DB2 10 new auditing capability to specific tables for specific programs during day**
  - Audit policy does not require AUDIT clause to be specified using DDL to enable auditing
  - Audit policy generate records for all read and 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 use new DB2 10 auditing capability to 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

New fine grain table controls to 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
- **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**

DB2 10 table controls to protect SQL access to individual rows

Establish a row policy for a table

- Filter rows out of answer set
- Policy can use session information, e.g. the SQL ID is in what group or user is using what role, to control which row is returned in result set
- Applicable to SELECT, INSERT, UPDATE, DELETE, & MERGE
- Defined as a row permission:

```
CREATE PERMISSION policy-name ON table-name
       FOR ROWS WHERE search-condition
       ENFORCED FOR ALL ACCESS ENABLE;
```

Optimizer inserts search condition in all SQL statements accessing table. If row satisfies search-condition, row is returned in answer set

Table controls to protect SQL access to individual column level

Establish a column policy for a table

- Mask column values in answer set
- Policy can use session information, e.g. the SQL ID is in what group or user is using what role, to control what masked value is returned in result set
- Applicable to the output of outermost subselect
- Defined as column masks :

```
CREATE MASK  mask-name ON table-name
   FOR  COLUMN  column-name RETURN CASE-expression
ENABLE;
```

Optimizer inserts CASE expression in all SQL statements accessing table to determine mask value to return in answer set

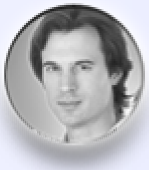
DB2 10 provides new ways to satisfy auditors

- ✓ 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

The need for database archiving:
For data retention, litigation hold and defensible disposal

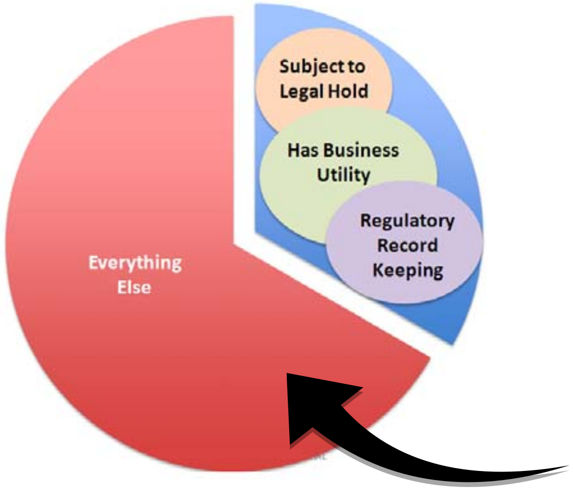
Legal

- Ensure information are retained and archived based on value and duration of value, containing risk
- Ensure litigation hold requirements are upheld
- Ensure defensibility of the consistent disposal of data records based guidelines and regulations



CIO

- Control IT costs while supporting business needs
- Oversee IT management and budget, including storage costs associated with data growth
- Balance data management costs and performance, while ensuring data retention, litigation hold and defensible disposal needs are met



You need a consistent, defensible solution to retain, preserve and eventually dispose enterprise data records, supporting both IT budget considerations & information governance decisions

InfoSphere Optim Data Growth Solution V8.1
What's New

- **Improved data warehouse performance through data growth management**
  - Native Teradata archiving capabilities for better performance

- **Enterprise archive bundle pricing to support enterprise-wide data growth initiatives**
  - Includes enterprise packaging and pricing for InfoSphere solutions to support the large enterprise's archiving and application retirement initiatives

- **Improved governance over your data with metering capabilities**
  - Measure the amount of data archived to document and understand storage ROI

- **Integration with ECM Atlas solutions**
  - Mitigate data retention, litigation hold, & disposal challenges of enterprise application data

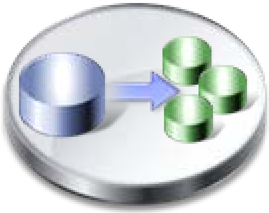
IBM InfoSphere Optim Enterprise Archive Edition
InfoSphere Optim Solutions packaged for the large enterprise

- **Enterprise archive bundle pricing to support enterprise-wide data growth initiatives**
  - Includes enterprise packaging and pricing for InfoSphere solutions to support the large enterprise’s archiving and application retirement initiatives

- **Offering includes InfoSphere Discovery, InfoSphere Optim Data Growth Solution & InfoSphere Option Solution for Application Retirement**

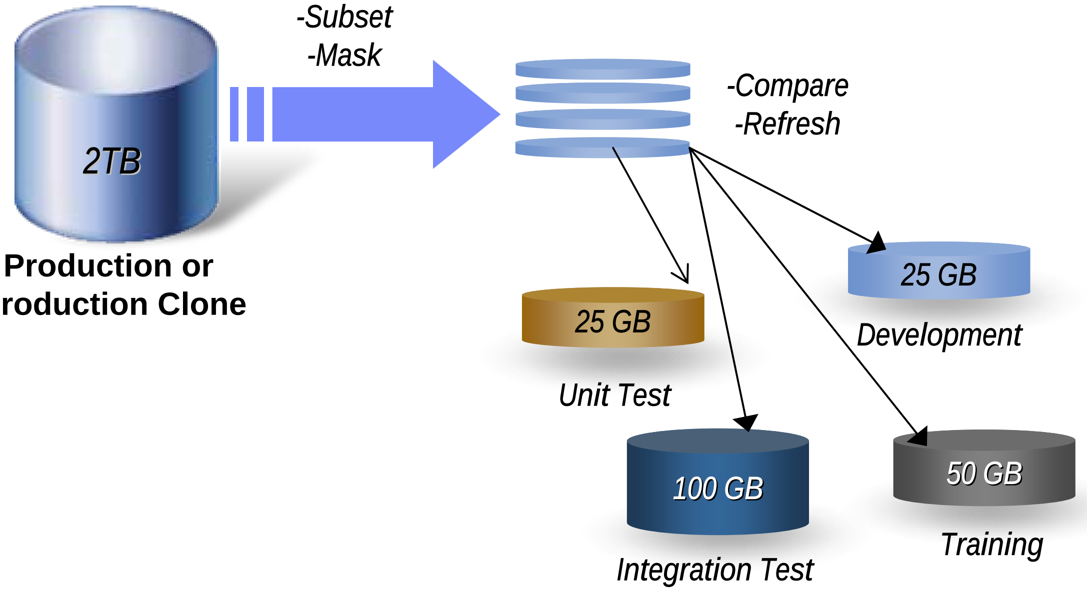
- **Chargeable components include InfoSphere Optim Data Find and accelerators for Oracle packaged applications**

IBM InfoSphere Optim Test Data Management Solution



Test Data Management

Create “right-size” production-like environments for application testing



InfoSphere Optim TDM supports data on distributed platforms (LUW) and z/OS.

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

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

Requirements

- Create referentially intact, “right-sized” test databases
- Automate test result comparisons to identify hidden errors
- Protect confidential data used in test, training & development
- Shorten iterative testing cycles and accelerate time to market

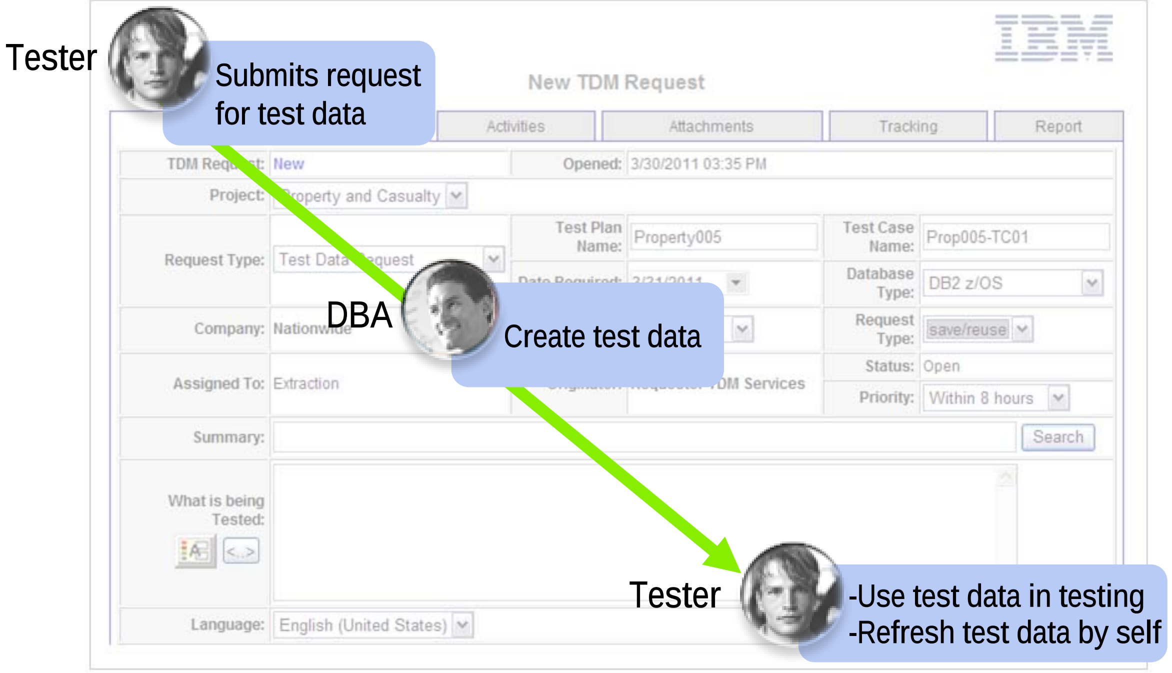
Benefits

- Deploy new functionality more quickly and with improved quality
- Easily refresh & maintain test environments
- Protect sensitive information from misuse & fraud with data masking
- Accelerate delivery of test data via self service center

IBM InfoSphere Optim Self Service Center for Test Data Management

Self Service Center

Streamline test data delivery



Tester

Submits request for test data

DBA

Create test data

Tester

-Use test data in testing
-Refresh test data by self

New TDM Request

TDM Request:	New	Opened:	3/30/2011 03:35 PM		
Project:	Property and Casualty				
Request Type:	Test Data Request	Test Plan Name:	Property005	Test Case Name:	Prop005-TC01
		Date Required:	3/31/2011	Database Type:	DB2 z/OS
Company:	Nationwide			Request Type:	save/reuse
Assigned To:	Extraction	Originator:	Requestor TDM Services	Status:	Open
				Priority:	Within 8 hours
Summary:					
What is being Tested:					
Language:	English (United States)				

Integrates with InfoSphere Optim Test Data Management Solution

Requirements

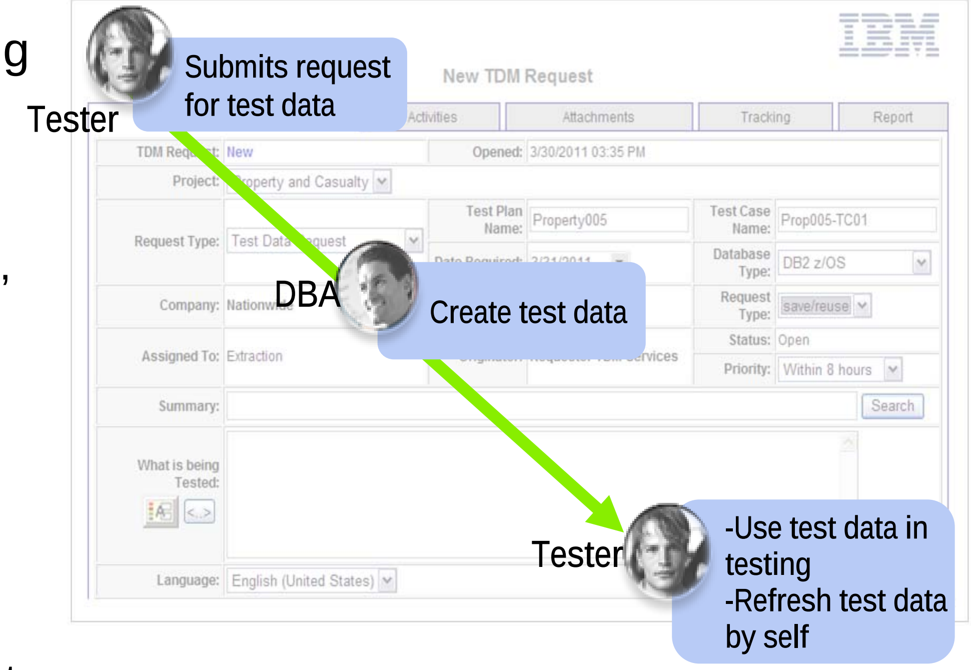
- Enable testers and developers to refresh test data
- Implement test data management process through a customizable and flexible workflow
- Understand status of test data environment

Benefits

- Streamlines test data refresh
- Improve visibility into test data management process
- Gain insight to make confident decisions

Govern test data management

- Implement customized test data management process, improving predictability and repeatability of testing efforts
  - Flexible test data management workflow
  - Provide role based access for testers, developers, DBAs, project managers etc
- Improve visibility into test data management process
  - Provide insight into the status of test data management requests
  - Integrates with InfoSphere Optim Test Data Management Solution to pull realistic test data for testing
  - Define and measure KPIs
  - Gain insight to make confident decisions



Tester: Submits request for test data

DBA: Create test data

Tester: -Use test data in testing
-Refresh test data by self

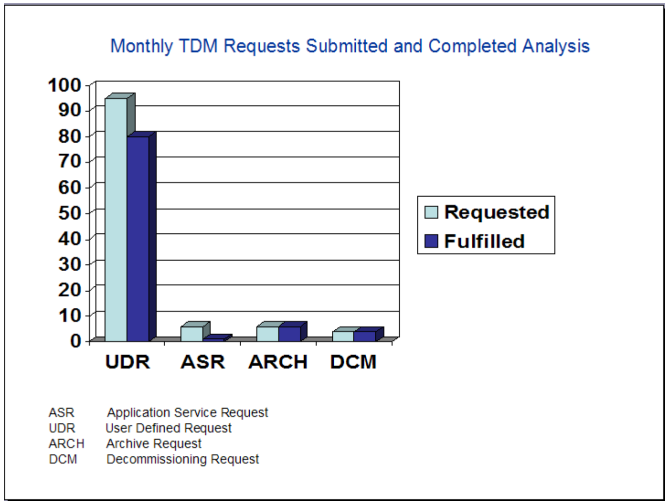
New TDM Request

TDM Request: New
Opened: 3/30/2011 03:35 PM
Project: Property and Casualty
Request Type: Test Data Request
Test Plan Name: Property005
Test Case Name: Prop005-TC01
Database Type: DB2 z/OS
Company: Nationwide
Request Type: save/reuse
Status: Open
Assigned To: Extraction
Priority: Within 8 hours
Summary:
What is being Tested:
Language: English (United States)

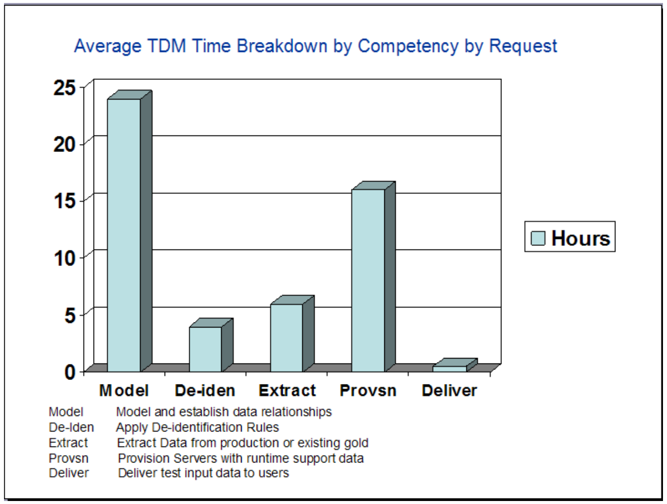
Gain insight to make confident decisions
Govern test data management

- **Run real-time reports on test data efficiency**
  - Test data management requests submitted and completed analysis
  - Average test data breakdown by competency by request

- **Run real-time reports on test data cost metrics**
  - Average test data management time breakdown by competency by request
  - Average test data management cost breakdown by competency by request



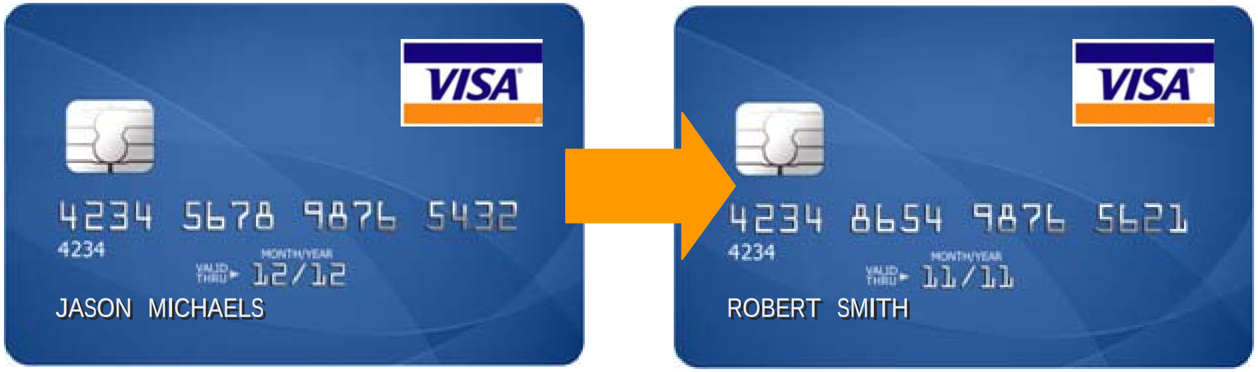
ASR	Application Service Request
UDR	User Defined Request
ARCH	Archive Request
DCM	Decommissioning Request



Model	Model and establish data relationships
De-Iden	Apply De-identification Rules
Extract	Extract Data from production or existing gold
Provsn	Provision Servers with runtime support data
Deliver	Deliver test input data to users

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.

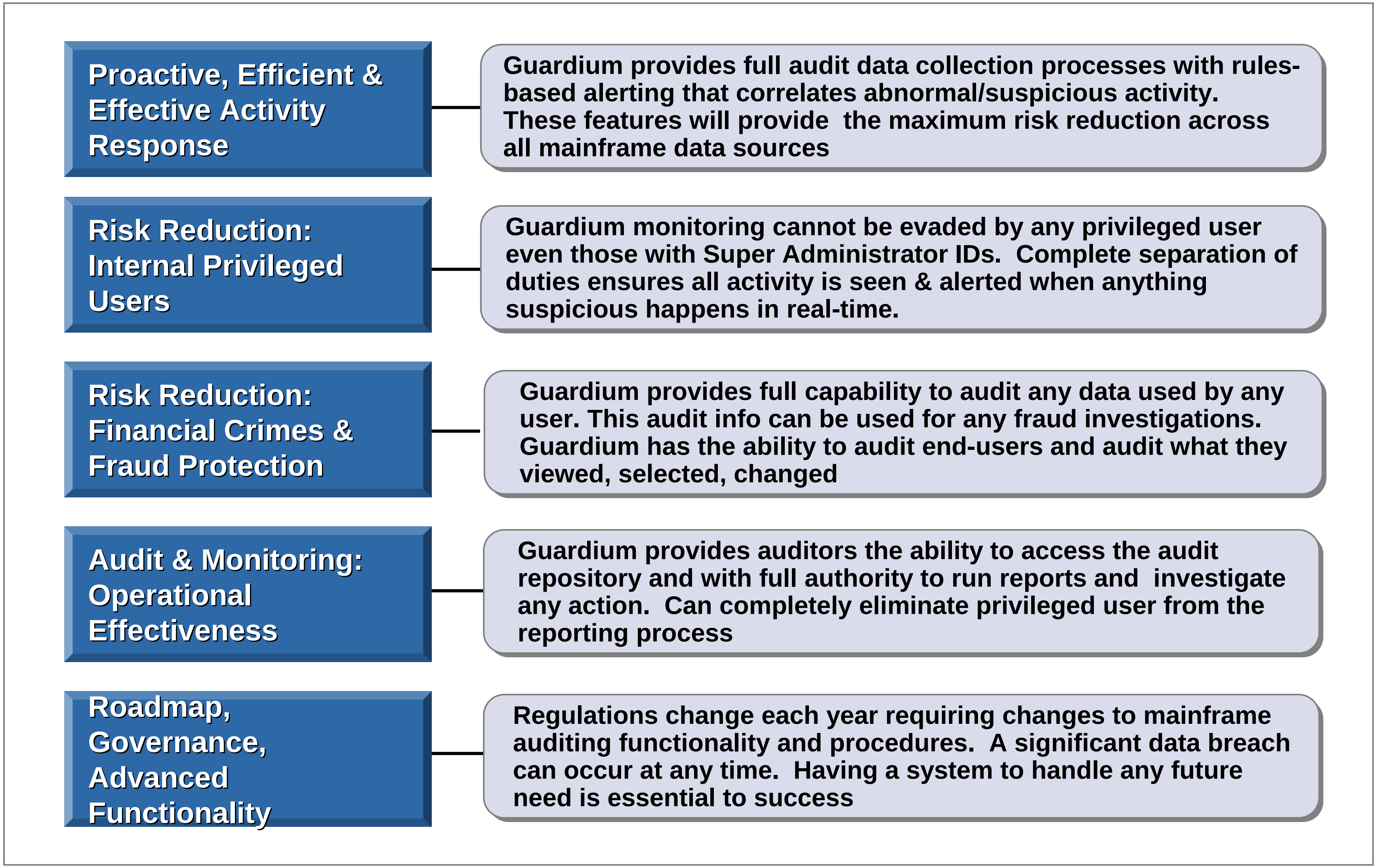
Requirements

- 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

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

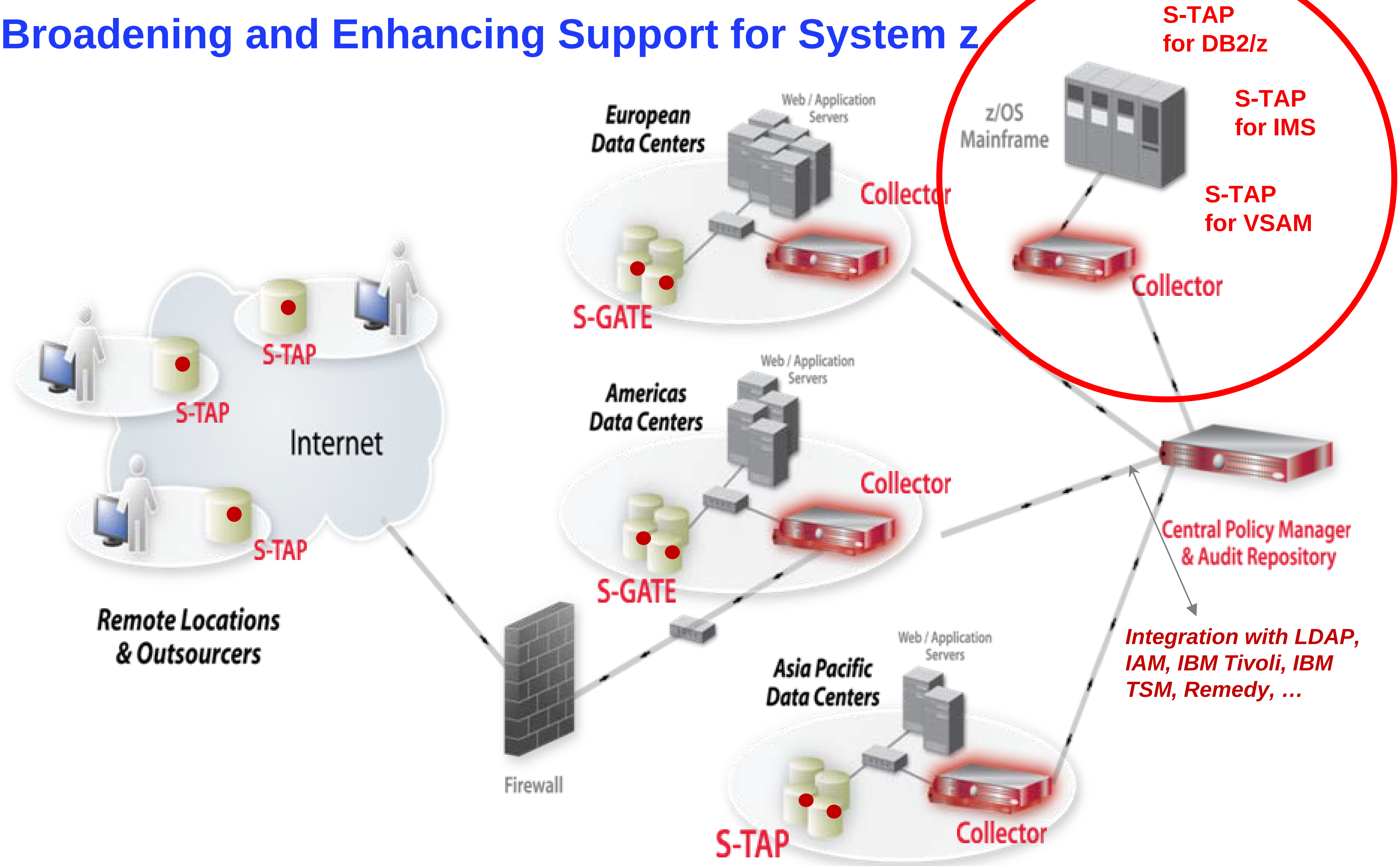
Roadmap, Governance, Advanced Functionality

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

InfoSphere Guardium BVA Top Security Enablers

- Real-Time Alerting: Intervene, investigate and prevent high risk events
- Central System Manager: Centralized Policy Management, Enforcement
- Violation & Alert Normalization: Limit the number of events
- Full Audit Trails / Forensics: Reduce the time to investigate alerts, violations
- Abnormal Behavior Detection: Detect high risk events even if no polices are violated
- Event Correlation: Detect seemingly unrelated suspicious activity as related
- CPU Utilization: Monitor all activity with minimal CPU utilization
- Disk Storage: High compression, Data aging rules, filtering keeps disk storage low
- Built-in Workflow: Automate violations with minimal intervention
- Vulnerability Assessment: 250+ out-of-the-box rules to determine vulnerabilities
- Confidential Data Discovery: Automate, discover and monitor key data elements
- Central Audit Data Repository: Report and BI for authorized users for reporting

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



Integration with LDAP, IAM, IBM Tivoli, IBM TSM, Remedy, …

Guardium for z

- **Provides a unified view and secure audit trail of all databa**
  - Across *both* mainframe and distributed environments
  - Enterprise-wide compliance reporting, alerting, analytics & forensics

- **Industry leading database activity monitor technology from Guardium**
  - Leverage all Guardium functionality off host

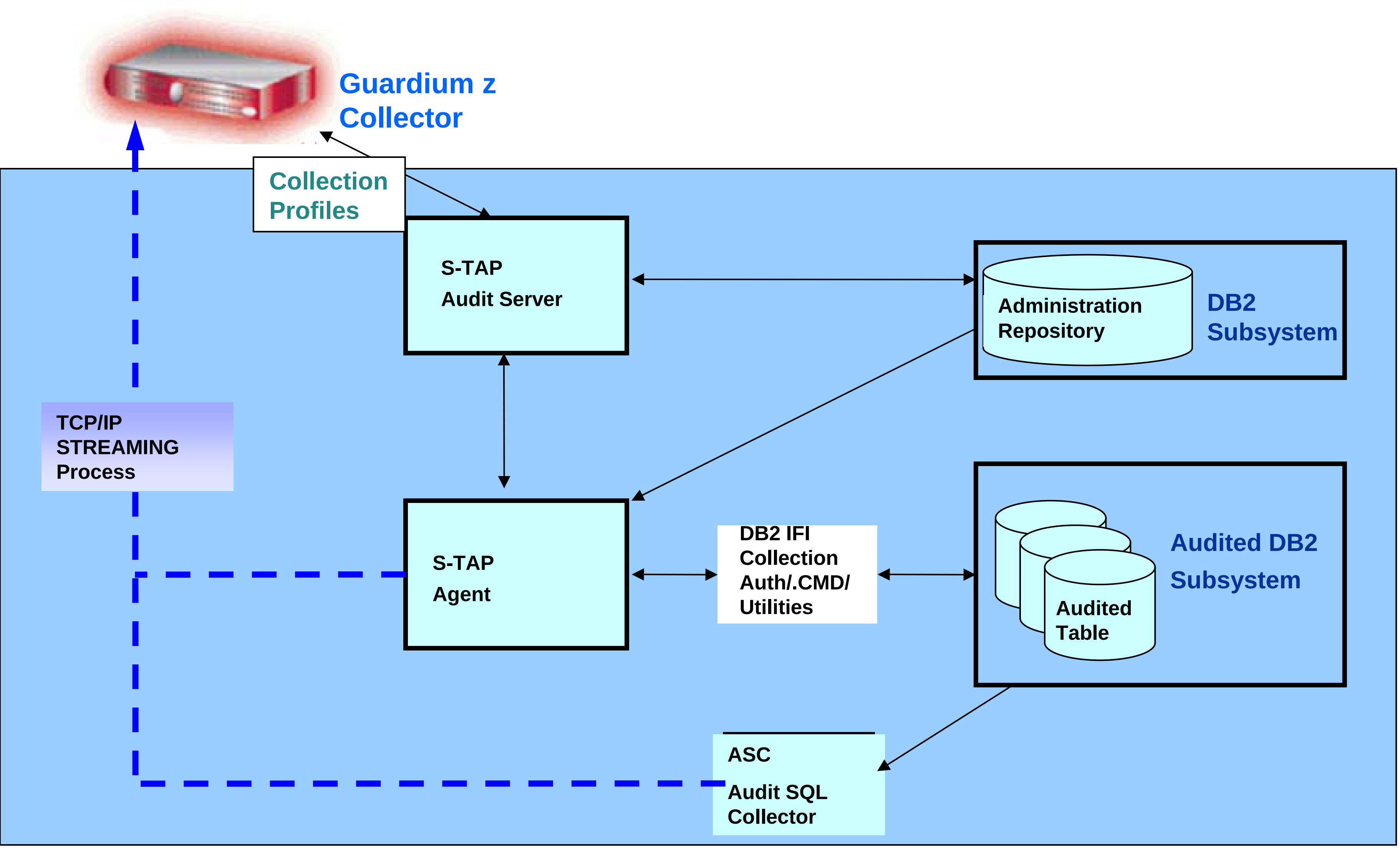
- **Best DB2/z event capture technology**
  - Lightweight deployment
  - DB2 trace not use for high volume SQL events
    - Class 3 / 4 / 5 audit traces NOT used
  - Ongoing performance and collection enhancements
  - Optimal performance for customers using IBM Query Monitor
    - Query Monitoring and Audit requirements leverage a single collector process

Guardium for z - Components

- **Guardium Collector appliance for System z**
  - Securely stores audit data collected by mainframe tap
  - 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
  - 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

Guardium S-TAP for DB2 on z/OS Architecture



Guardium z Collector

Collection Profiles

S-TAP
Audit Server

Administration Repository

DB2 Subsystem

TCP/IP STREAMING Process

S-TAP
Agent

DB2 IFI Collection Auth/.CMD/ Utilities

Audited Table

Audited DB2 Subsystem

ASC

Audit SQL Collector

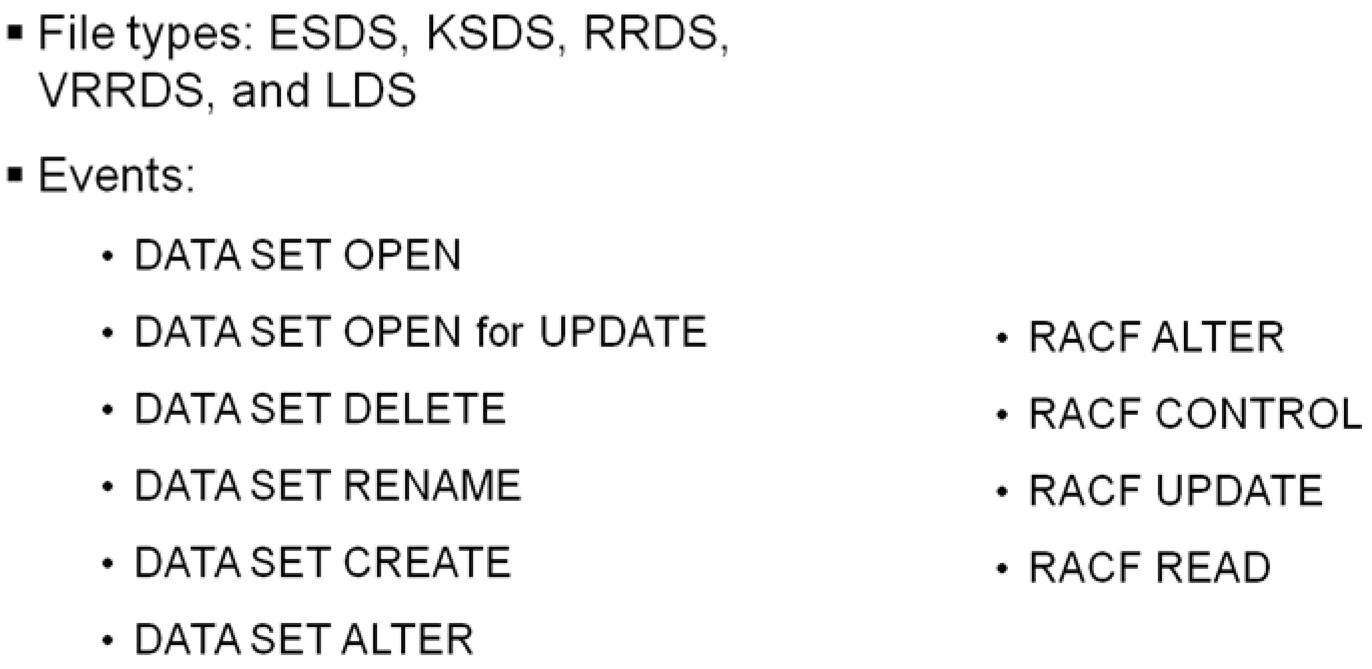
Guardium S-TAP for IMS on z/OS

- **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 S-TAP for collecting VSAM event

•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 Vulnerability Assessment
Based on best practices

- **New capability to 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

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 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)

Thank
You