Data Security and Protection on IMS: Are you ready for the next Audit?

Session 16716

Dennis Eichelberger - deichel@us.ibm.com
Marilene Roder – marilene@us.ibm.com

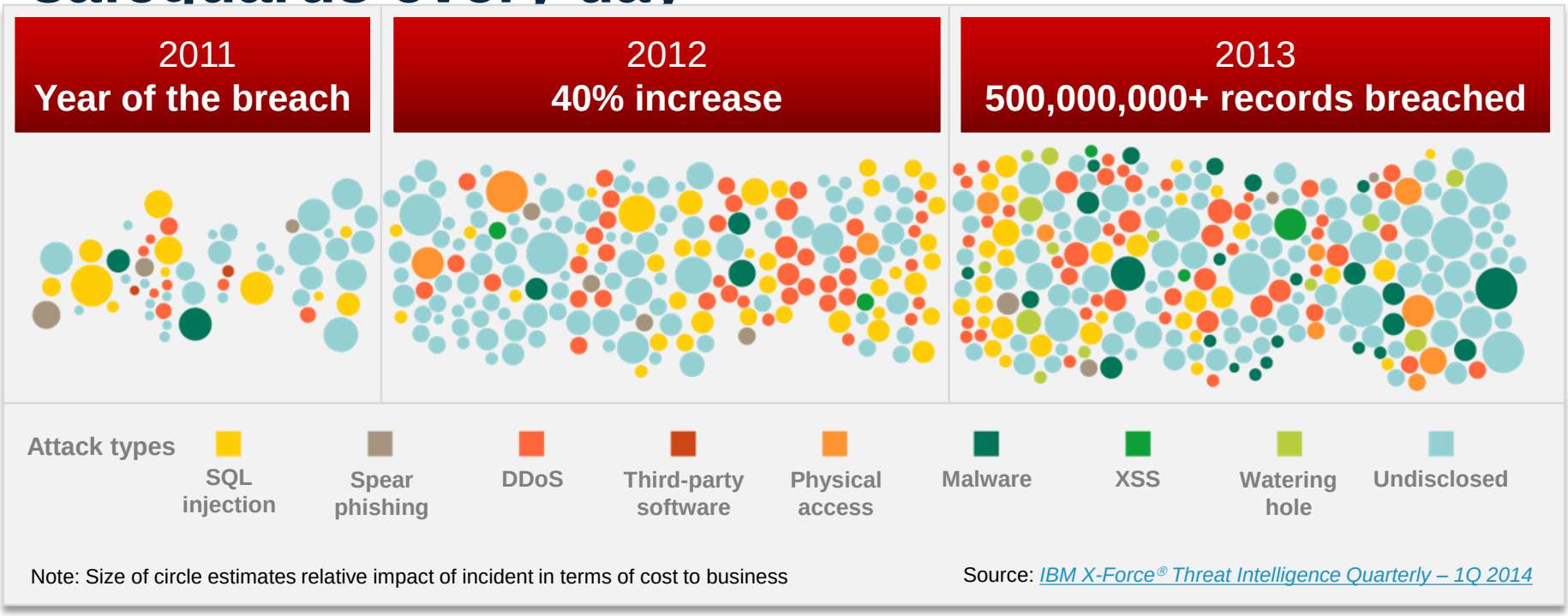
#SHAREorg

SHARE is an independent volunteer-run information technology association that provides education, professional networking and industry influence.

SHARE in Seattle 2015


Really?
You know? You can
do this online now.
PEVEY

Sophisticated attackers break through safeguards every day



Note: Size of circle estimates relative impact of incident in terms of cost to business

Source: *IBM X-Force® Threat Intelligence Quarterly – 1Q 2014*

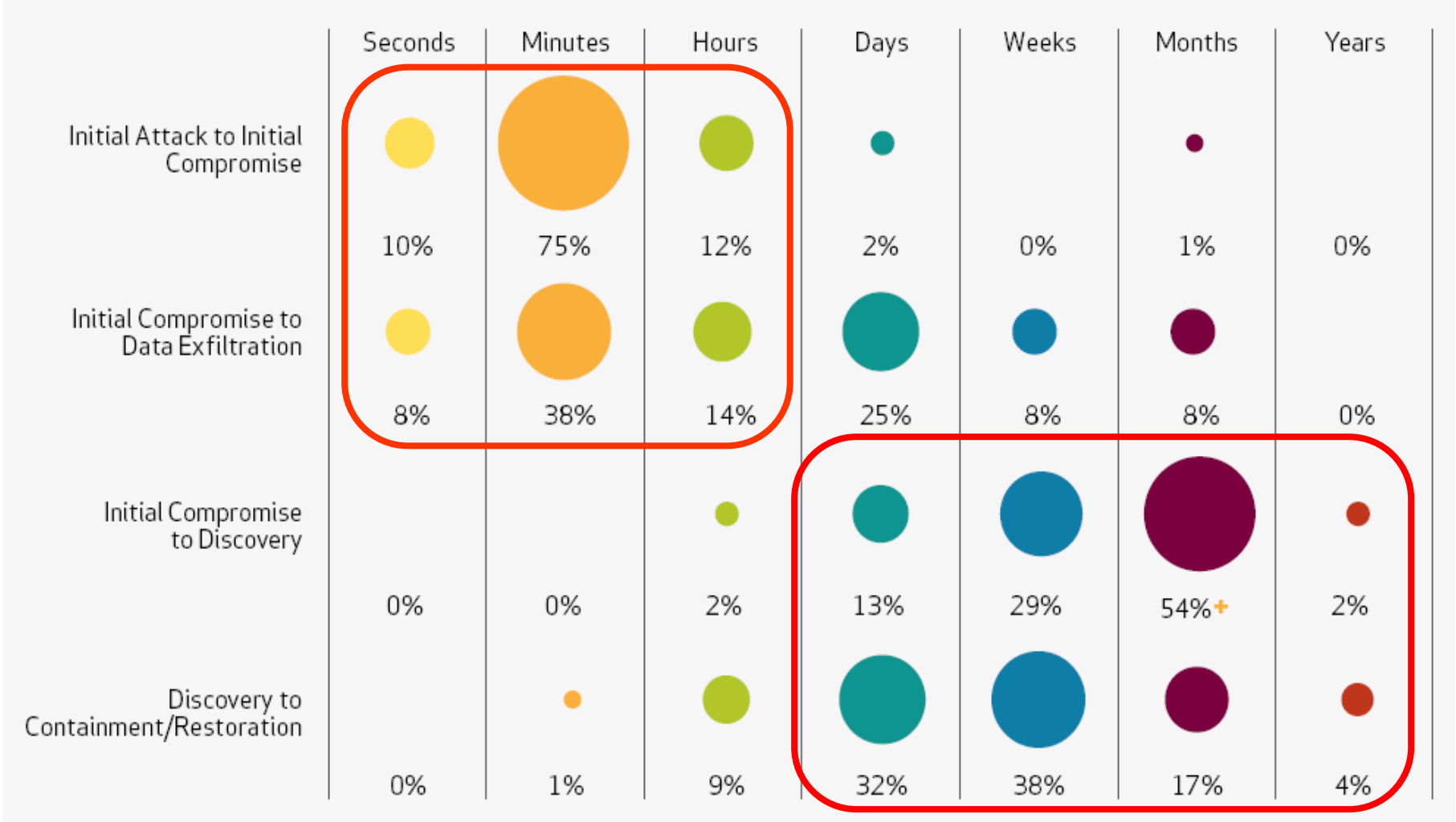
61% of organizations say **data theft and cybercrime** are their greatest threats

2012 IBM Global Reputational Risk & IT Study

$3.5M+ average cost of a **data breach**

2014 Cost of Data Breach, Ponemon Institute

Compromises Take Weeks and Months to Discover



http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf?CMP=DMC-SMB_Z_ZZ_ZZ_Z_TV_N_Z038

Data is the key target for security breaches….. … and Database Servers Are The Primary Source of Breached Data

Table 10. Compromised assets by percent of breaches and percent of records*

Type	Category	All Orgs		Larger Orgs	
POS server (store controller)	Servers	50%	1%	2%	<1%
POS terminal	User devices	35%	<1%	2%	<1%
Desktop/Workstation	User devices	18%	34%	12%	36%
Automated Teller Machine (ATM)	User devices	8%	<1%	13%	<1%
Web/application server	Servers	6%	80%	33%	82%
Database server	Servers	6%	96%	33%	98%
Regular employee/end-user	People	3%	1%	5%	<1%
Mail server	Servers	3%	2%	10%	2%
Payment card (credit, debit, etc.)	Offline data	3%	<1%	0%	<1%
Cashier/Teller/Waiter	People	2%	<1%	2%	<1%
Pay at the Pump terminal	User devices	2%	<1%	0%	<1%
File server	Servers	1%	<1%	5%	<1%
Laptop/Netbook	User devices	1%	<1%	5%	<1%
Remote access server	Servers	1%	<1%	7%	<1%
Call Center Staff	People	1%	<1%	7%	<1%

WHY?

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

2012 and 2013 Data Breach Report from Verizon Business RISK Team

http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

"Web application and database servers form another logical grouping, and once again account for most of the records breached. That makes sense because, well, those assets store a lot of records."

Mainframe customers are more vulnerable to security incidents

Key concerns

50% concerned with privileged insiders

21% concerned with advanced persistent threats

29% concerned with web-enabled z/OS apps

"As mainframes become a major component in service-oriented architectures, they are increasingly exposed to malware. Web services on the mainframe have significantly impacted security."

Meenu Gupta
President, Mittal Technologies Inc.

of customers agree that deploying

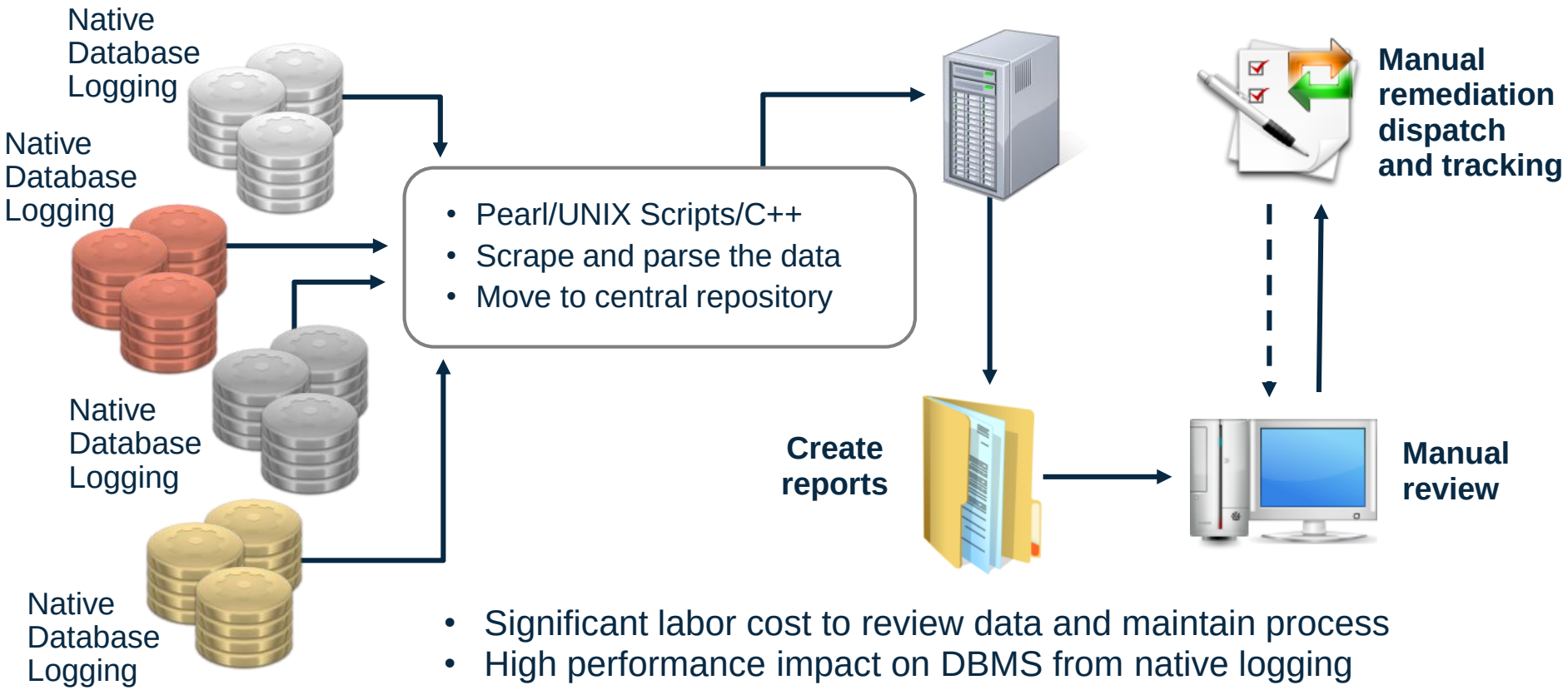
provides the best mainframe protection

Source: IBM Webinar 2/6/2014, Security Intelligence Solutions for System z and the Enterprise

But System z is already secure - why do we need more?

- Separation of duties
  - Privileged users “need to know” vs abuse or mistake
  - Trace-based auditing controlled by privileged users
  - SAF plays a vital role in protection of data on z/OS, but is not tamper-resistant and actionable
- Achieving audit readiness is labor-intensive and introduces latency
  - RACF lacks sufficient granularity for reporting
  - IMS logging is real time, But reporting of that information is usually ‘after the fact’
- Real time vs. batch processing
  - Batch processing of audit data from external sources prevents real time alerting

Typical Home Grown Solutions Are Costly and Ineffective



- Significant labor cost to review data and maintain process
- High performance impact on DBMS from native logging
- Not real time
- Does not meet auditor requirements for Separation of Duties
- Audit trail is not secure
- Inconsistent policies enterprise-wide

Data at Rest Encryption on z/OS

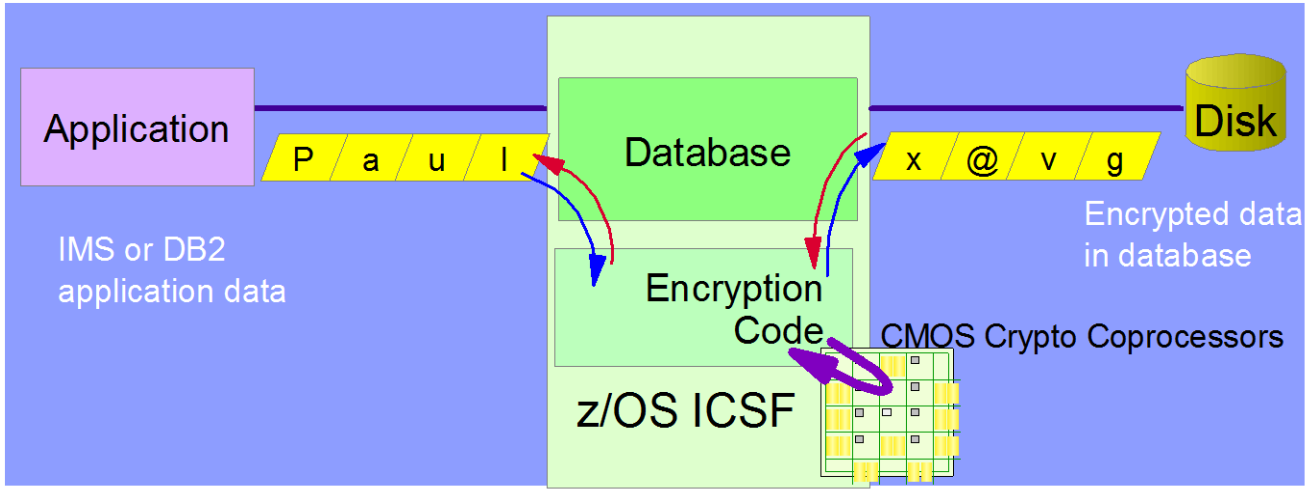
Guardium Data Encryption for DB2 and IMS Databases

#SHAREorg

SHARE is an independent volunteer-run information technology association that provides **education**, professional **networking** and industry **influence**.

SHARE in Seattle 2015

Data Encryption for DB2 and IMS



- Supports all levels of DB2 & IMS
- No application changes needed
- Applications need no awareness of keys
- Supports both secure key and clear key encryption
- Index access is unaffected by encryption
- Compatible with IMS Load/Unload utilities and IMS Tools

- Data encryption on disk
- Data on channel is encrypted (protects against channel/network sniffers)
- Existing authorization controls accessing this data are unaffected
- Assumption made that access is through the DBMS, or, direct access invokes the DBMS data exits

Encryption and “Data at Rest” Protection

- Requirement: How to protect “data at rest” to ensure that it is only accessed for business need-to-know?
- Consider the following scenario:
  - Linear VSAM datasets are controlled via RACF from direct access outside of database subsystems via dataset access rules
  - DBA or Storage Administrator has RACF authority to read VSAM datasets in order to perform legitimate storage administration activities.
  - Administration privileges can be abused to read the linear VSAM datasets directly and access clear-text data outside of RACF protections.
- Now consider the above scenario, but with the underlying Linear VSAM datasets encrypted
  - When DBA or Storage Administrator uses their RACF dataset authorities in a manner which is outside of business need-to-know, the data retrieved is cybertext and thus remains encrypted and protected.
  - Only way to access and obtain clear-text data will be via DLI which can be protected via IMS / RACF interface

Encryption Algorithms – Which Ones Are Best?

- DES (Data Encryption Standard)
  - 56-bit, viewed as weak and generally unacceptable today by the NIST
- TDES (Triple Data Encryption Standard)
  - 128-bit, universally accepted algorithm
- AES (Advanced Encryption Standard)
  - 128- or 256- bit, newest commercially used algorithm
- What is acceptable?
  - DES is viewed as unacceptable
  - TDES is viewed as acceptable and compliant with NIST (National Institute of Standards and Technology)
  - AES 128 or 256 is also viewed as acceptable and strategic

InfoSphere Guardium Data Encryption for DB2 and IMS Databases

- **Implementation uses COMPRTN keyword, on SEGM statement of DBD Generation**
  - Acceptable overhead when accessing any column in table
  - No Additional Security
  - Database must be unloaded and reloaded to add COMPRTN
  - Keys may be encrypted
  - Data encrypted in place
  - Application Transparent

InfoSphere Guardium Data Encryption for DB2 and IMS Databases

- **Existing implementation uses DB2 EDITPROC for row level encryption**
  - Acceptable overhead when accessing any column in table
  - No Additional Security
  - Table must be dropped and reloaded to add EDITPROC
  - Indexes not encrypted
  - Application Transparent

- **New Functionality Fieldproc**
  - Same basic characteristics as EDITPROCs

InfoSphere Guardium

In-depth Data Protection

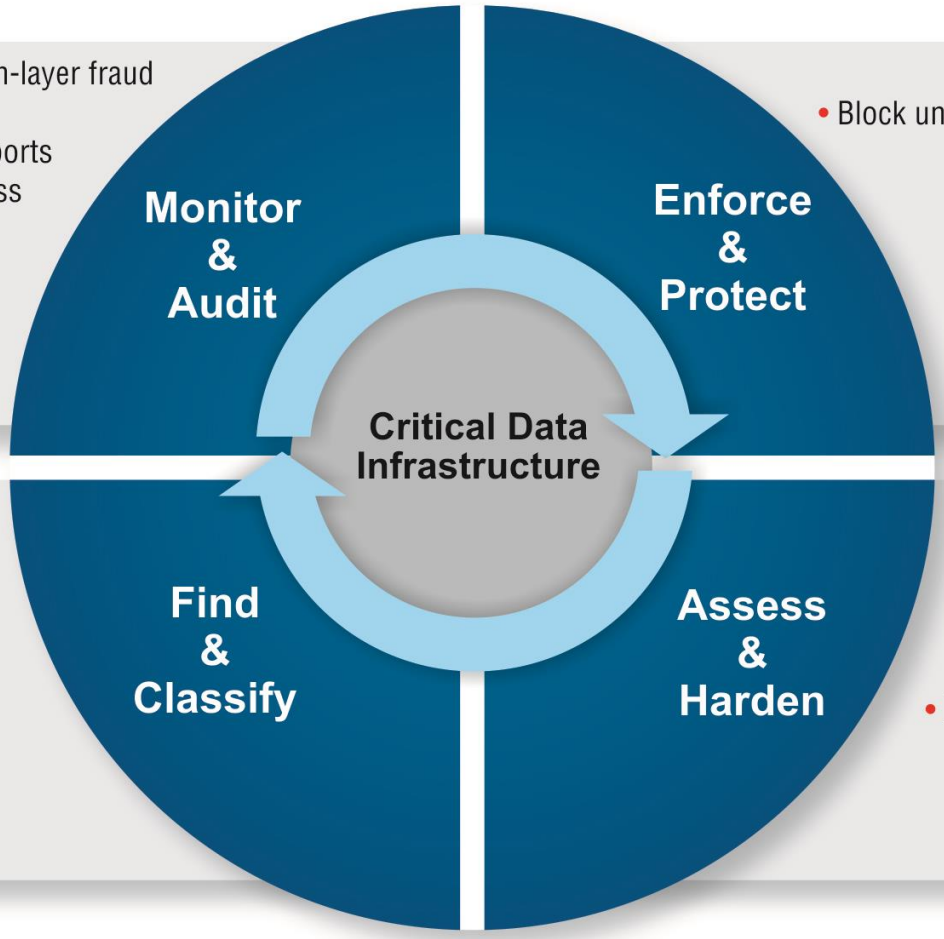
#SHAREorg

SHARE is an independent volunteer-run information technology association that provides **education**, professional **networking** and industry **influence**.

SHARE in Seattle 2015

Addressing the full data security and compliance lifecycle

- Detect cyber attacks & application-layer fraud
- Monitor privileged users
- Detailed “audit-ready” activity reports
- Centralized audit repository - cross DBMS, unstructured & Hadoop
- Built-in compliance workflow
- SIEM Integration
- Pre-configured policies & reports



- Prevent cyber attacks
- Block unauthorized access to sensitive data
- Enforce change control
- Quarantine suspicious users
- Mask sensitive data
- Control firewall ids

- Discover data sources
- Classify sensitive data
- Automate security policies
- Automate compliance reports

- Assess database vulnerabilities - static and behavioral
- Map predefined tests to best-practice standards (STIG, CIS, CVE)
- Monitor entitlements and database credentials
- Alert on configuration changes

How we do it?

Data at Rest

Discovery Classification

Masking Encryption

Configuration Data

Vulnerability Assessment

Entitlements Reporting

Data in Motion

Activity Monitoring

Blocking Quarantine

Dynamic Data Masking

Where is the sensitive data?

How to protect sensitive data?

How to secure the repository?

Who should have access?

What is actually happening?

How to prevent unauthorized activities?

How to protect sensitive data to reduce risk?

Security Policies

Dormant Data

Security Alerts / Enforcement

Dormant Entitlements

Compliance Reporting

InfoSphere Guardium Value Proposition:

Continuously monitor access to sensitive data including databases, data warehouses, big data environments and file shares to….

1 Prevent data breaches

- Prevent disclosure or leakages of sensitive data

2 Ensure the integrity of sensitive data

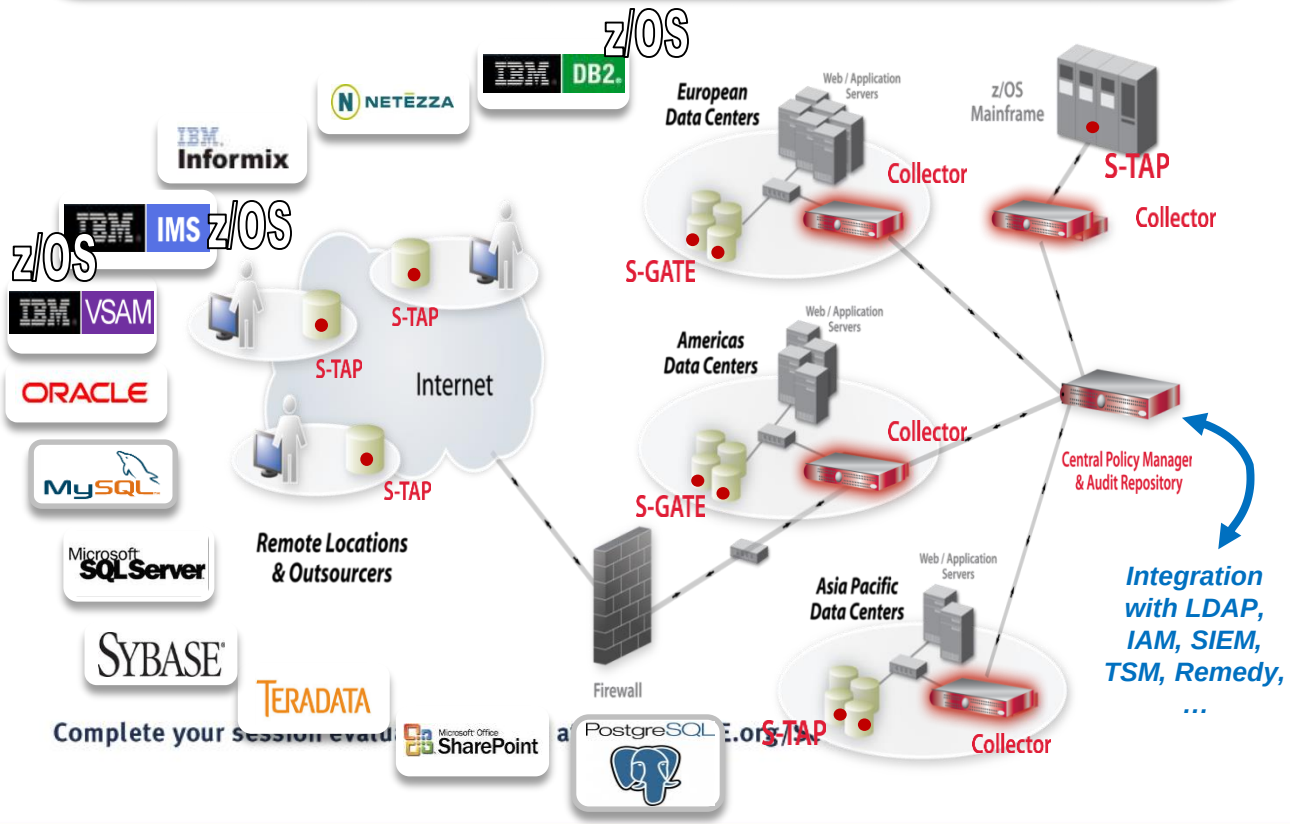
- Prevent unauthorized changes to data, database structures, configuration files and logs

3 Reduce cost of compliance

- Automate and centralize controls
  - Across diverse regulations, such as PCI DSS, data privacy regulations, HIPAA/HITECH etc.
  - Across heterogeneous environments such as databases, applications, data warehouses and Big Data platforms like Hadoop
- Simplify the audit review processes

IBM Guardium Provides Real-Time Database Security & Compliance

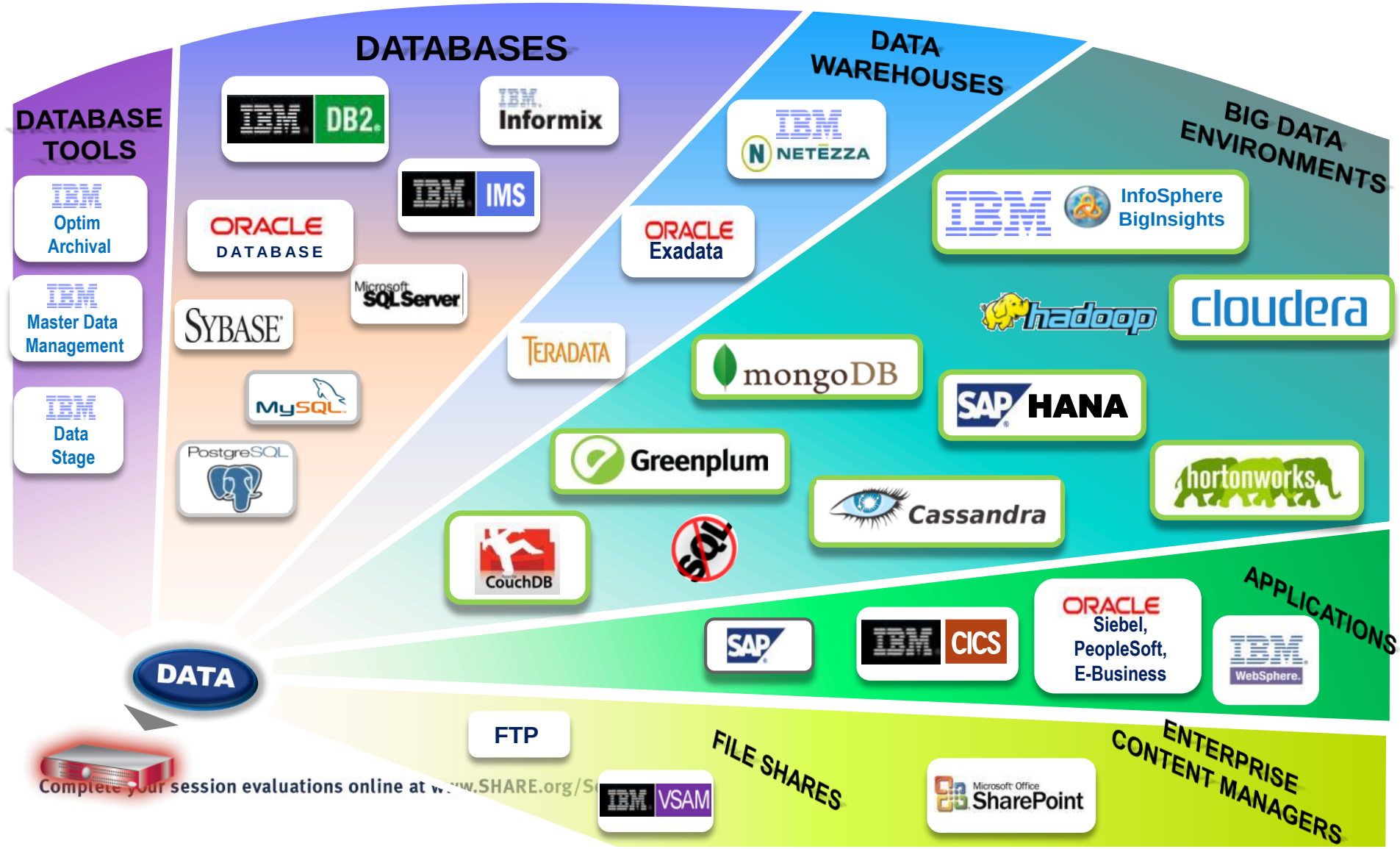
- ✓ **Continuous, policy-based, real-time monitoring of all database activities, including actions by privileged users**
- ✓ **Database infrastructure scanning for missing patches, misconfigured privileges and other vulnerabilities**
- ✓ **Data protection compliance automation**



Key Characteristics

- Single Integrated Appliance
- Non-invasive/disruptive, cross-platform architecture
- Dynamically scalable
- SOD enforcement for DBA access
- Auto discover sensitive resources and data
- Detect unauthorized & suspicious activity
- Granular, real-time policies
  - *Who, what, when, how*
- Prepackaged vulnerability knowledge base and compliance reports for SOX, PCI, etc.
- Growing integration with broader security and compliance management vision

Extend real-time Data Activity Monitoring to also protect sensitive data in data warehouses, Big Data Environments and file shares

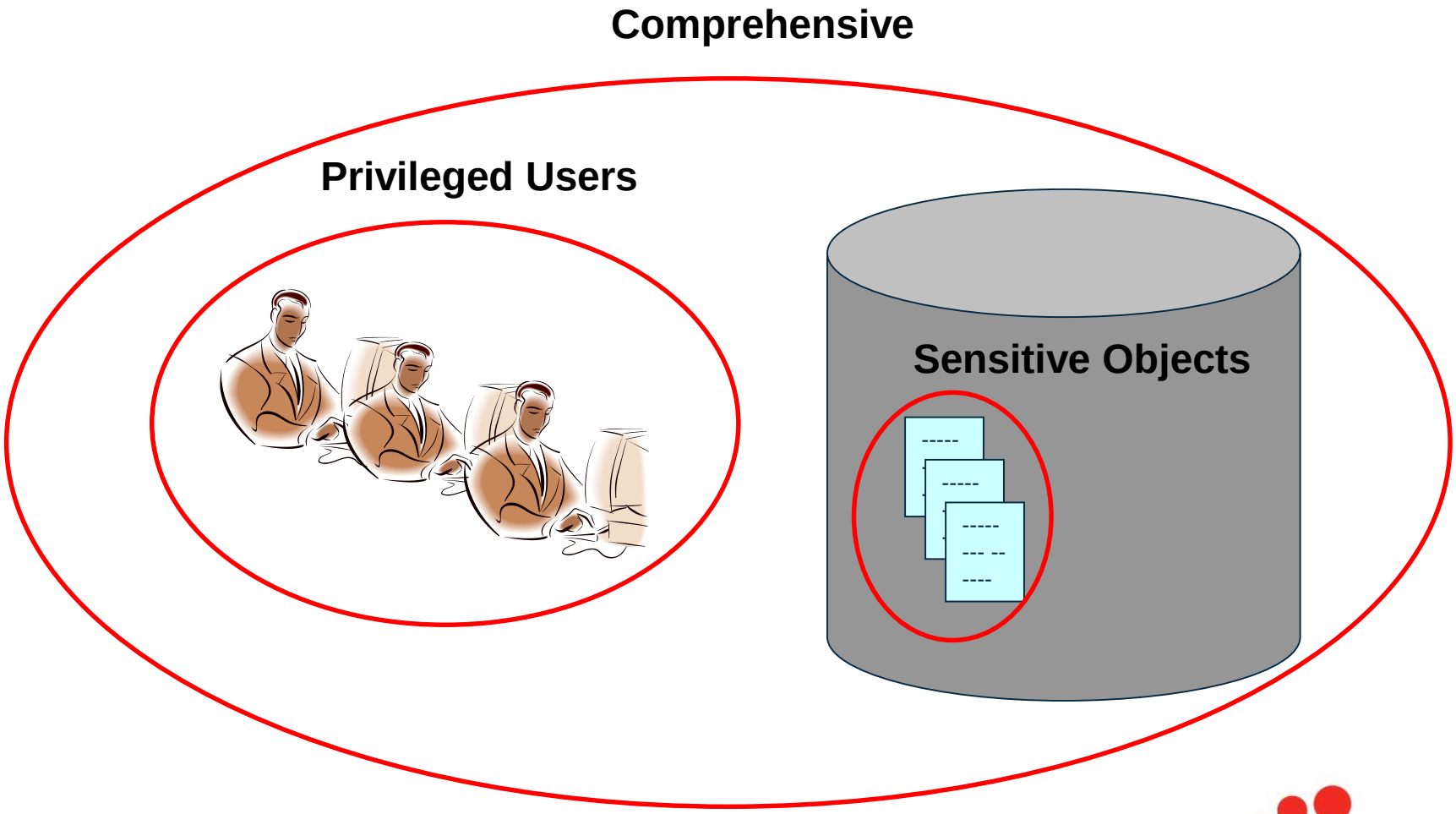


InfoSphere Guardium:
Guardium for System z

Guardium for System z - Components

- **Guardium Collector appliance for System z**
  - Securely stores audit data collected by mainframe S-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, IMS or Data Sets) 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
  - Audit data streamed to appliance – small mainframe footprint

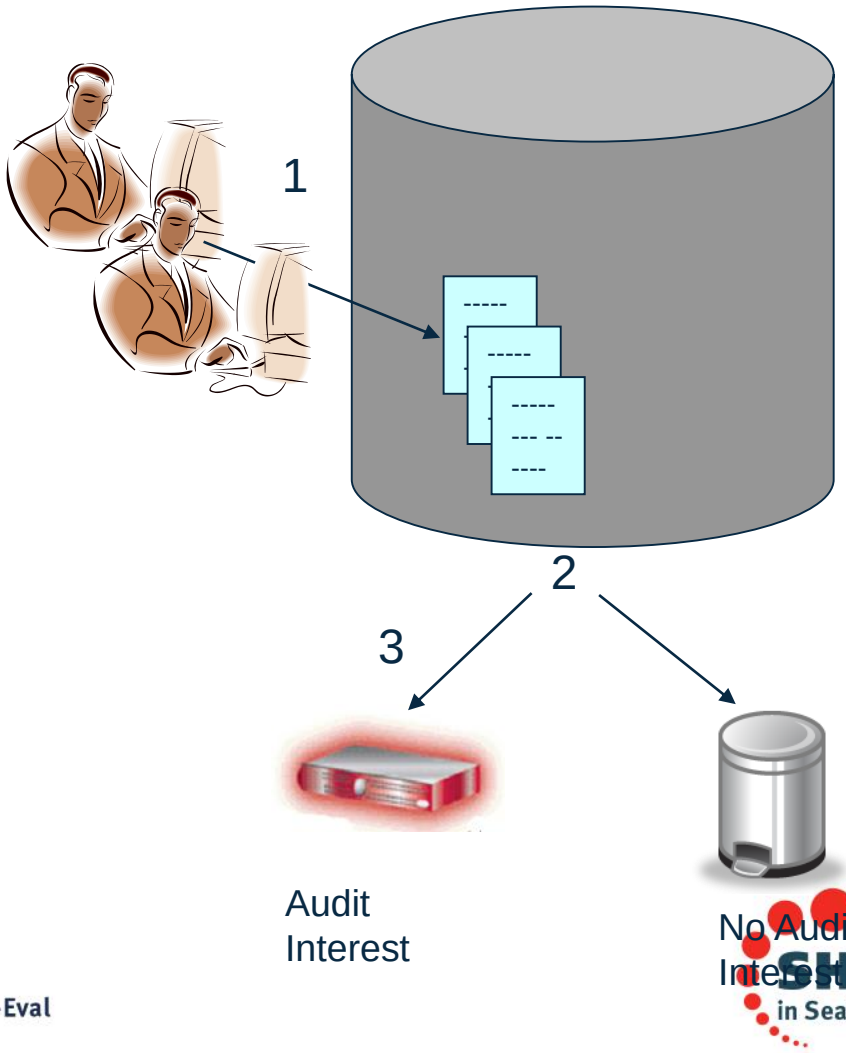
Monitoring with Guardium on System z



Complete control over what is audited

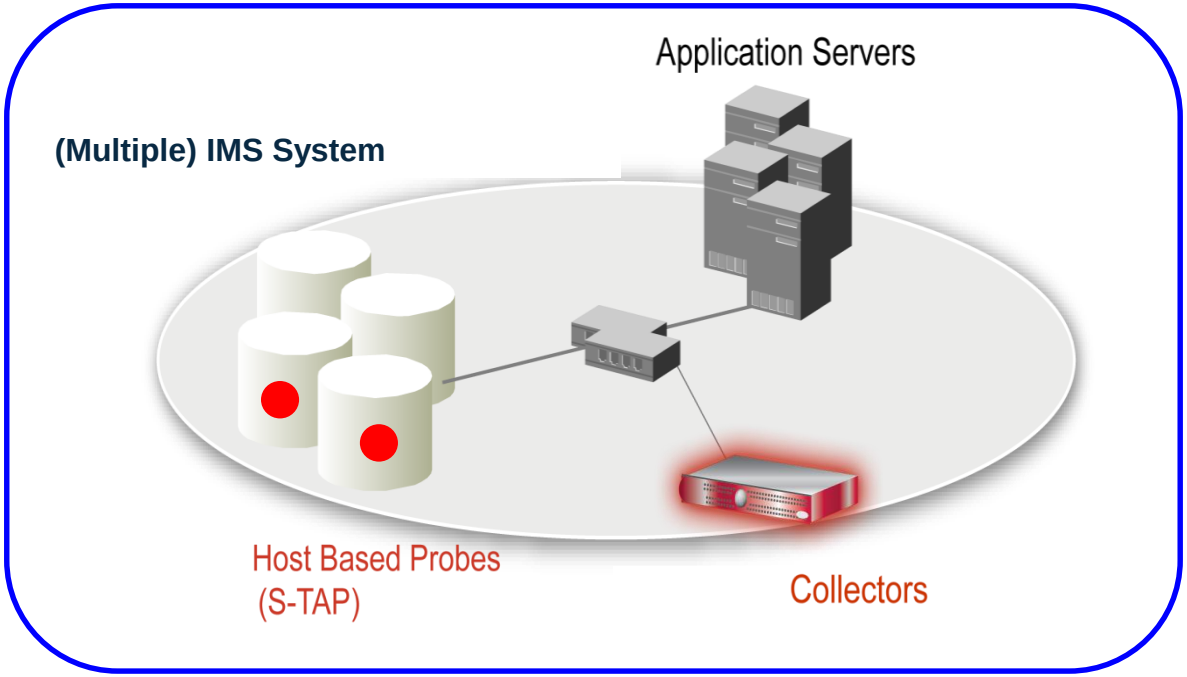
Three key components for Guardium on System z

1. **Data Gathering**
   - Collecting each SQL or DLI statement
2. **Data Filtering**
   - Determining if the SQL or DLI statement matches a monitoring policy
3. **Data Movement**
   - Packaging and sending the SQL or DLI call and call content to the Guardium collector



InfoSphere Guardium:
Guardium for IMS on System z

IBM InfoSphere Guardium S-TAP for IMS on z/OS V9.1



- 4 Sources to collect audit information:
  - IMS Online regions (DLIO DLIB)
  - IMS DLI/DBB batch jobs
  - SMF (System Management Facility)
  - IMS Archive Log (SLDS)

IBM InfoSphere Guardium S-TAP for IMS on z/OS V9.1

- S-TAP for IMS's function is to collect Audit information of access to IMS Databases and IMS artifacts
- Audit Data Collected
  - Accesses to databases and segment
    - IMS Online regions
    - IMS DLI/DBB batch jobs
    - INSERT (ISRT), UPDATE (REPL), DELETE,(DLET) and GET
    - Obtain concatenated key and segment data
    - Links Get Hold and Replace calls which enables before and after images of UPDATED segments

- Support for zIIP Processors: IMS S-TAP V9.0 adds zIIP support from within an IMS Online Control Region

What “non-IMS” Data is Collected?

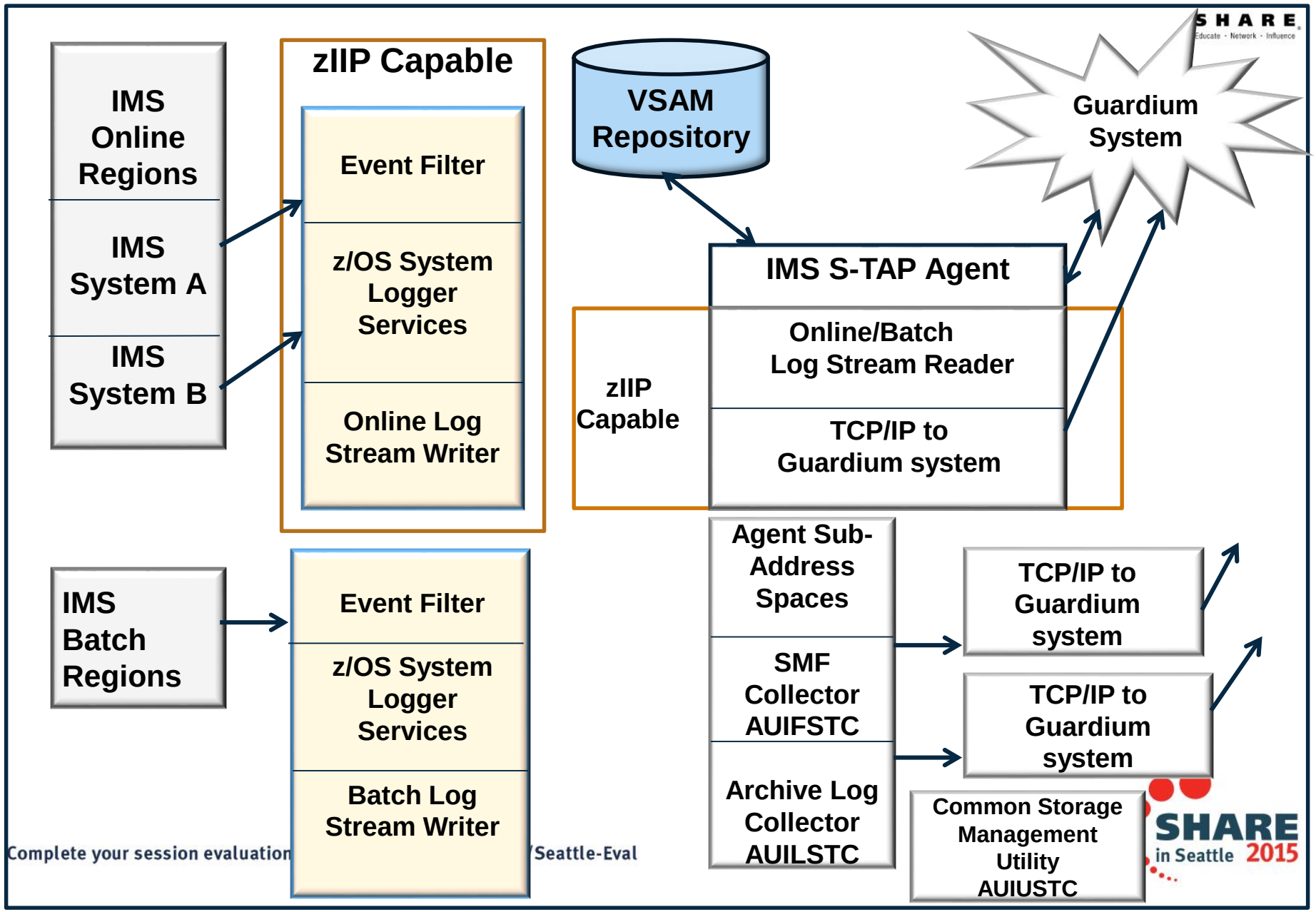
Access to IMS related information outside the control of IMS services

- Database data sets
- Image copy data sets
- IMS log data sets
- RECON data sets.
- RENAMES: records and reports the original DSN and the new DSN
- User access to the IMS system via SIGNON as recorded in the IMS log
- PSB and database (DBD) ‘change of state’ activity as recorded in the IMS log
  - Displayed as an EVENT with pertinent (PSB name, DBD name, DBD name, USERID, etc.
  - System STOP and START activity as recorded in the IMS log
- IBM utility access:
  - from IMS Batch (DLI/DBB/BMP) jobs and IMS Online regions

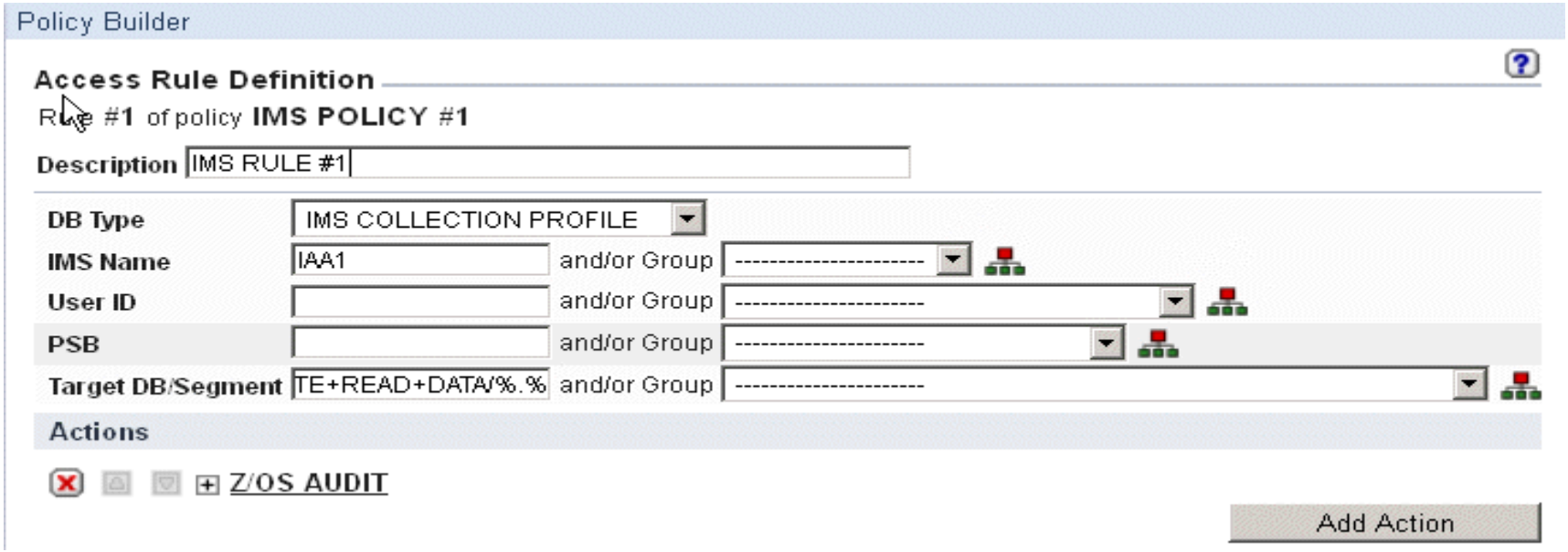
Guardium S-TAP for IMS Version 9.1 Features

- Architectural changes
  - Windows based Administration GUI has been discontinued
  - Configuration Screens added to G System screens
  - Server Address space AUISssid has been eliminated
  - Keywords added in the Agent configuration file
- Expanded zIIPs processor support
- S-TAP Log Messages available to view from Guardium - System
- The agent configuration file syntax has been modified
- Internal architecture changes

Guardium S-TAP for IMS V 9.1 Architecture



IMS Collection Policy Definition



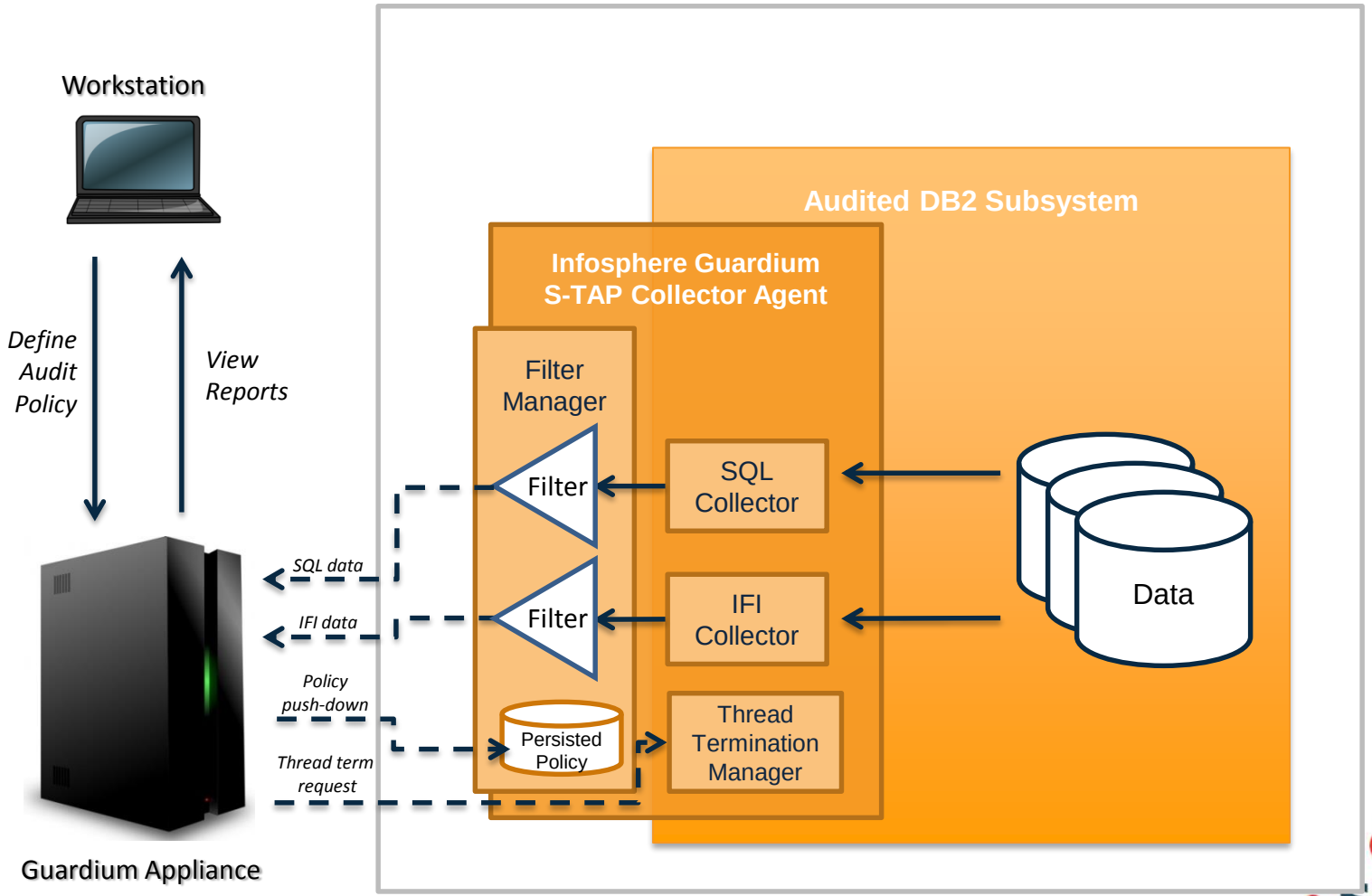
- **User ID** – INCLUDE/'user id' or 'mask', Blank defaults to Include all
  - EXCLUDE can be used in Groups to refine INCLUDE mask
- **PSB** – INCLUDE/PSB name' or 'mask', Blank defaults to Include all
  - EXCLUDE can be used in Groups to refine INCLUDE mask

InfoSphere Guardium:
Guardium for DB2 on System z

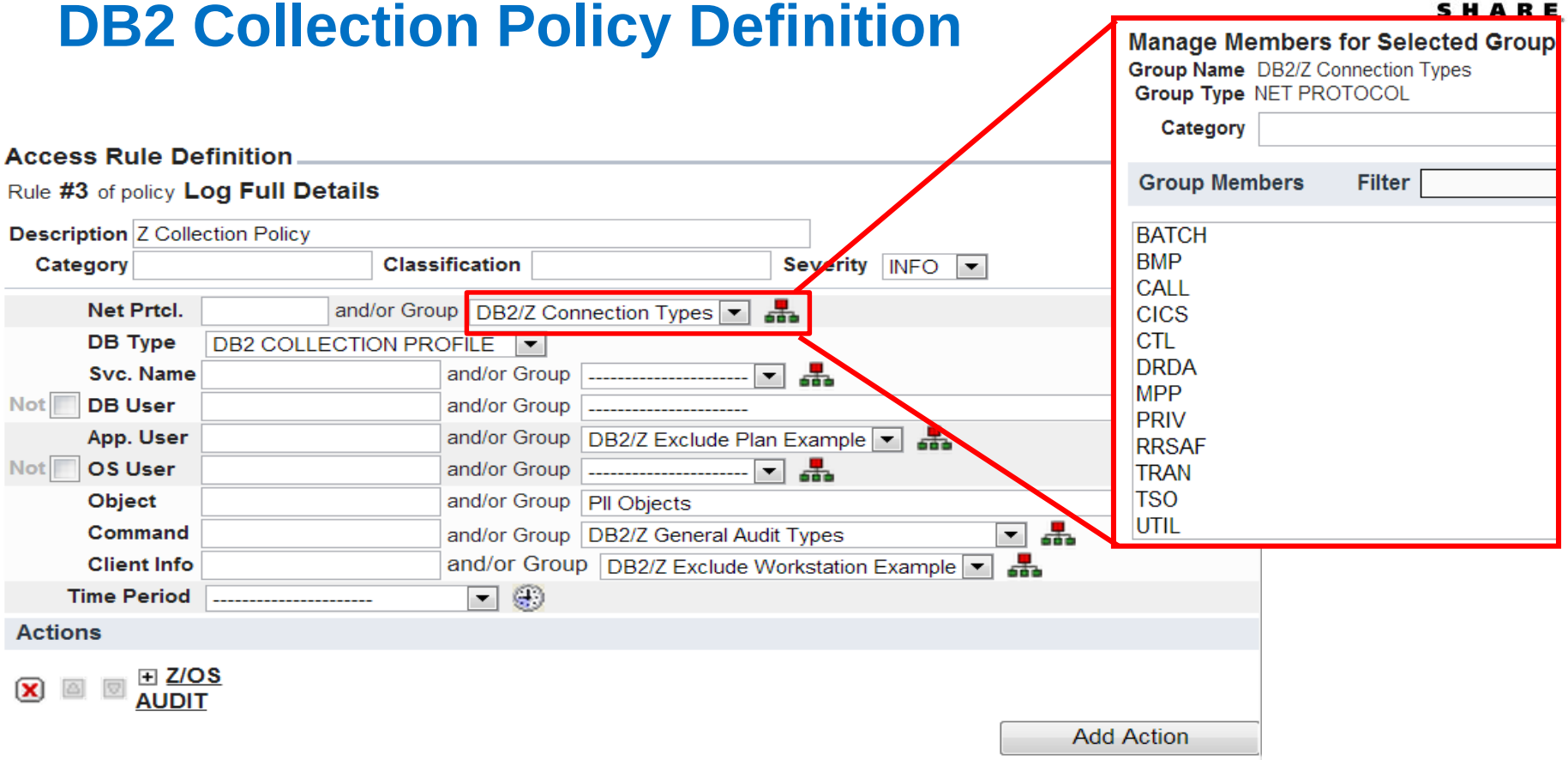
Guardium for DB2 z/OS Version 9.1 Features

- Capture of all database activities on DB2 for z/OS by privileged users, mainframe resident applications, and network clients, including those connecting via services such as JDBC or DB2 Connect
- Capture of critical operations such as SELECTs, DML, DDL, GRANTS, and REVOKES
- Direct streaming of audit data from z/OS process to a networked Guardium appliance to support near real-time reporting
- Flexible filtering of which events should be captured to help manage data volume and performance overhead
- Centralized interaction through the Guardium appliance
- zIIP Eligible processes are available
- Greater resilience against network and appliance outages through the use of the failover and spill file features, along with Policy Persistence, to enable audit data collection to continue in the event of an appliance outage
- Continued performance improvements

Guardium S-TAP for DB2 on z/OS V9.1 Architecture



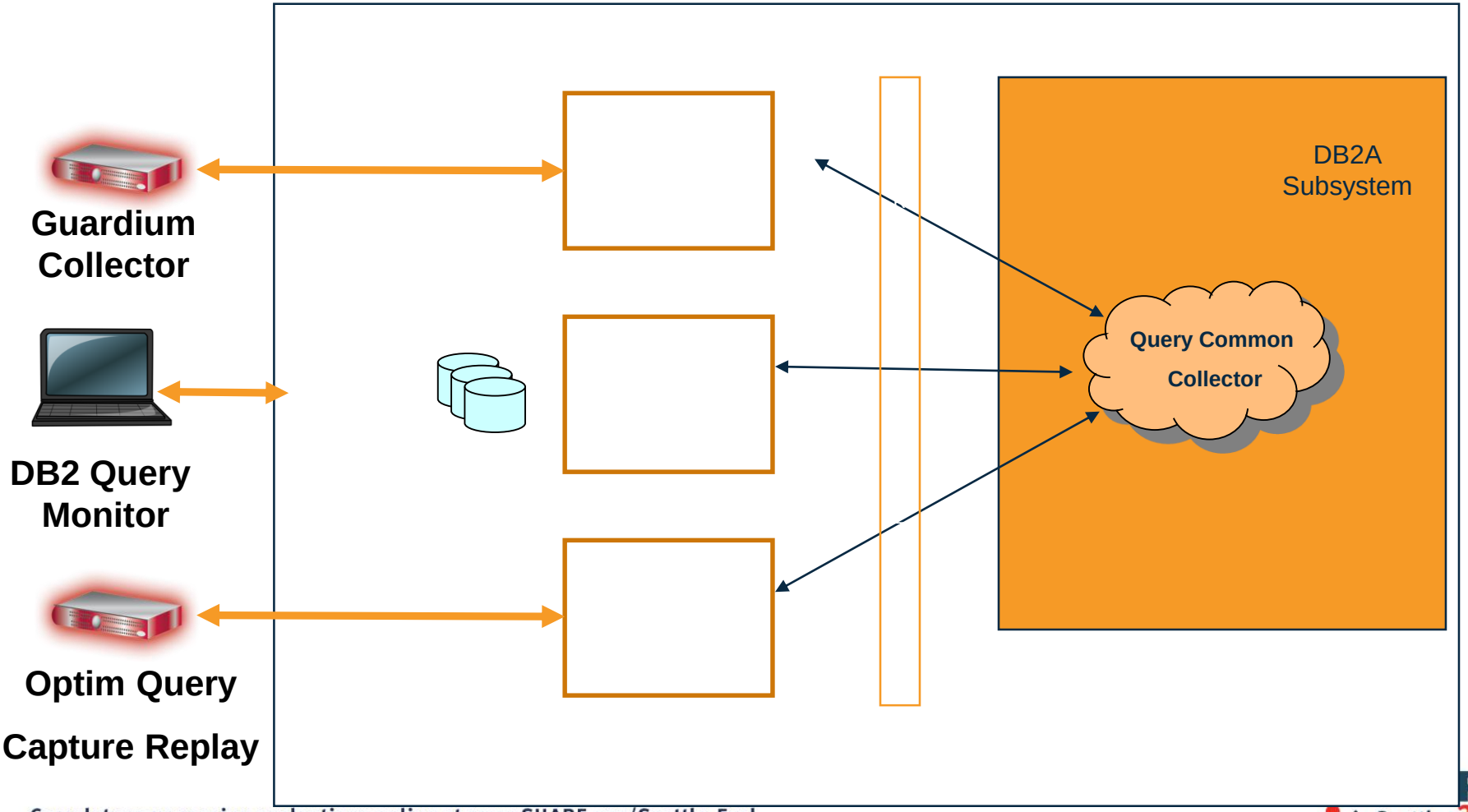
DB2 Collection Policy Definition



- Granular Controls over connection type
- Connection types can easily be included or excluded
- Connection type filtering is very efficient

Huge Advantage of Query Common Collector

minimum resources / minimum overhead / maximum usability (Only pay once for collection process)

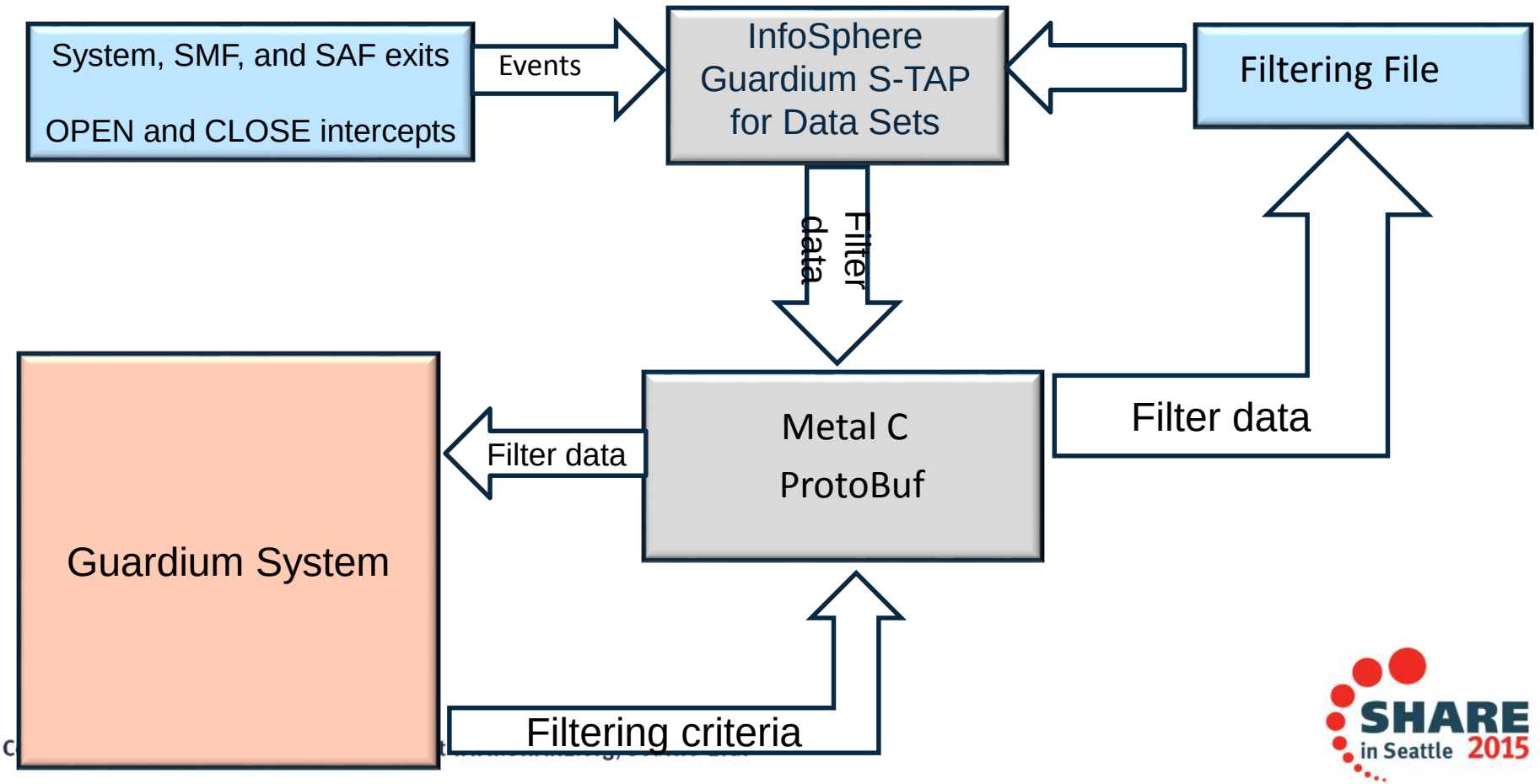


InfoSphere Guardium:
Guardium for Data Sets on System z

Guardium S-TAP for Data Sets Version 9.1 Features

- Name change - S-TAP for Data Sets on z/OS
- Improved time-to-reporting for Data Set Level Events
- Monitoring of non-VSAM data sets
- CICS Component for Record Level Monitoring of VSAM data sets
- CICS SIGNON file access identification
- Syntax of Control File changed to provide a more consistent feel across the various STAPs

Data Set S-TAP V9.1 Architecture



Name change - S-TAP for Data Sets on z/OS

- **IBM InfoSphere Guardium S-TAP for VSAM V9.0 has been re-named**

- **IBM InfoSphere Guardium S-TAP for Data Sets V9.1 (PID: 5655STX)**
  - Includes enhancements made to the 9.0 version of the product
  - Includes new features and function requested by customers
    - Faster Event capture – no waiting for the SMF Type 30 record
    - VSAM and Non-VSAM data set monitoring
    - CICS component for Record Level Monitoring of VSAM data sets

Improved time-to-reporting for Data Set Level Events

- **Previous version of S-TAP for Data Sets (VSAM) required SMF Type 30 records to monitor data before reporting events**
  - Type 30 records are closure records for a job
    - When the type 30 end-of-job is encountered, SMF data is then collected and saved, ‘closed out', and sent to the Guardium appliance
    - In the case of long running tasks, this process may require a significant duration of time
  - This caused delays in reporting data set level events for long-running tasks until they went through step or job termination
- **S-TAP for Data Sets collects the necessary data without waiting for the SMF Type 30 record**
  - This is accomplished by obtaining the data previously provided by the SMF Type 30 records at the time of event creation, resulting in event reporting at the same time as the event occurs
- **Immediate reporting**
  - You no longer must wait until a CICS address space terminates, or a TSO user logs off

Monitoring of non-VSAM Data Sets

- **The following file types continue to be monitored for VSAM**
  - ESDS KSDS RRDS VRRDS LDS
- **The following file types will be monitored for non-VSAM**
  - PS (Physical sequential)
  - PO (Partitioned organization)
  - DA (Direct Access)
  - PDSE (Partitioned Data Set Extended)
- **The following events will be monitored for non-VSAM**
  - DATA SET CREATE
  - DATA SET CLOSE
    - Data set was accessed for input
    - Data set was accessed for output
  - DATA SET DELETE
  - DATA SET RENAME
  - Security (SAF) DEFINE, READ, UPDATE, ALTER and CONTROL violations

InfoSphere Guardium

Guardium Data Encryption for DB2 & IMS databases

Guardium S-TAP for Data Sets on z/OS

Guardium S-TAP for DB2 on z/OS

Guardium S-TAP for Data Sets on z/OS

Thank You