IBM SolutionsConnect 2013
Turning Opportunity into Outcomes.

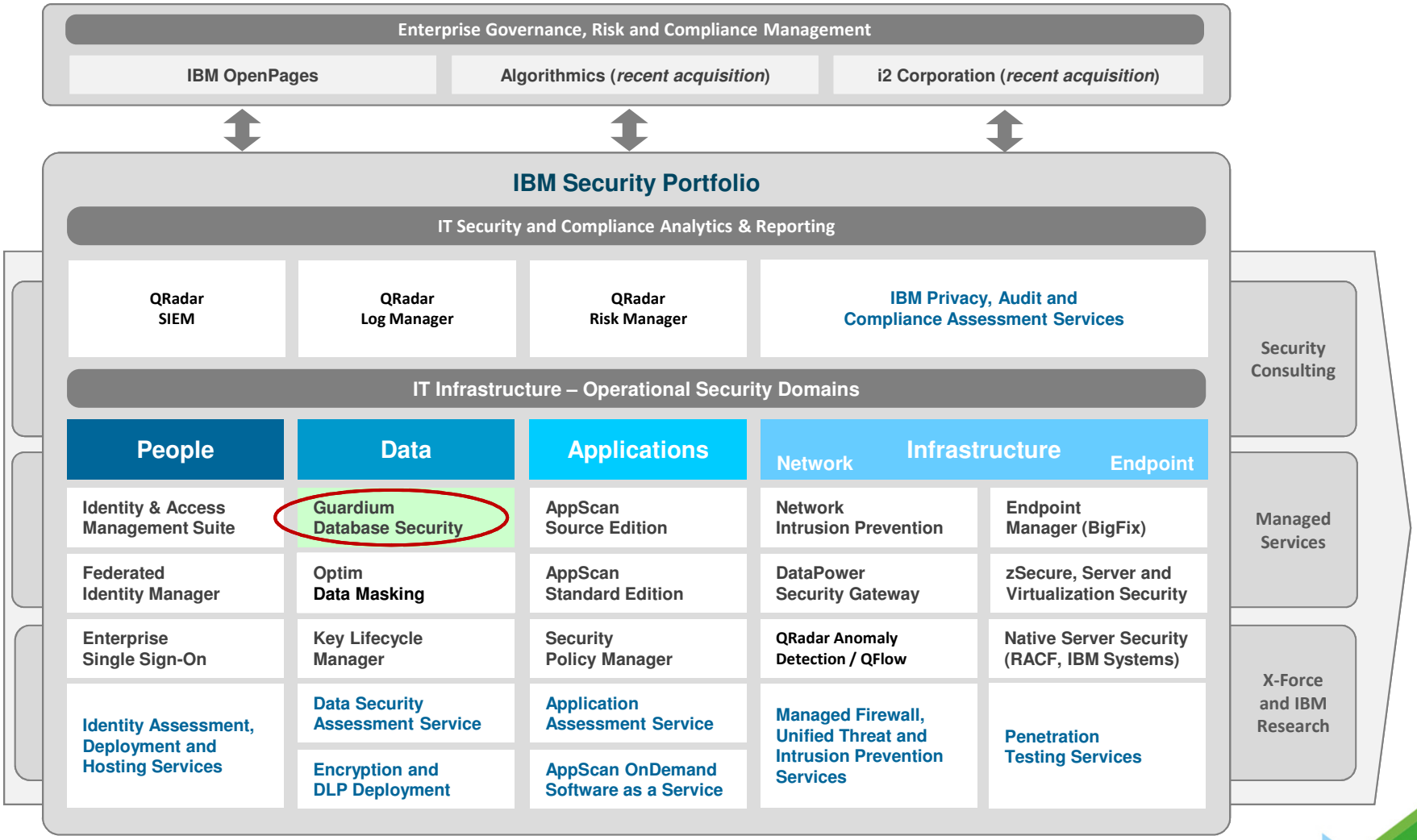
Database security and auditing

How to protect your most valuable assets and meet compliance requirements

Fakhreddine EL Mourabiti
fmourabiti@be.ibm.com


You know? you can do this online now.
P.C.VEY

InfoSphere Guardium in IBM IT Security Portfolio



360 º strategic view

Heterogeneous RDBMS

(Oracle, DB2, Netezza, Informix, Sybase, Sun MySQL, Teradata)

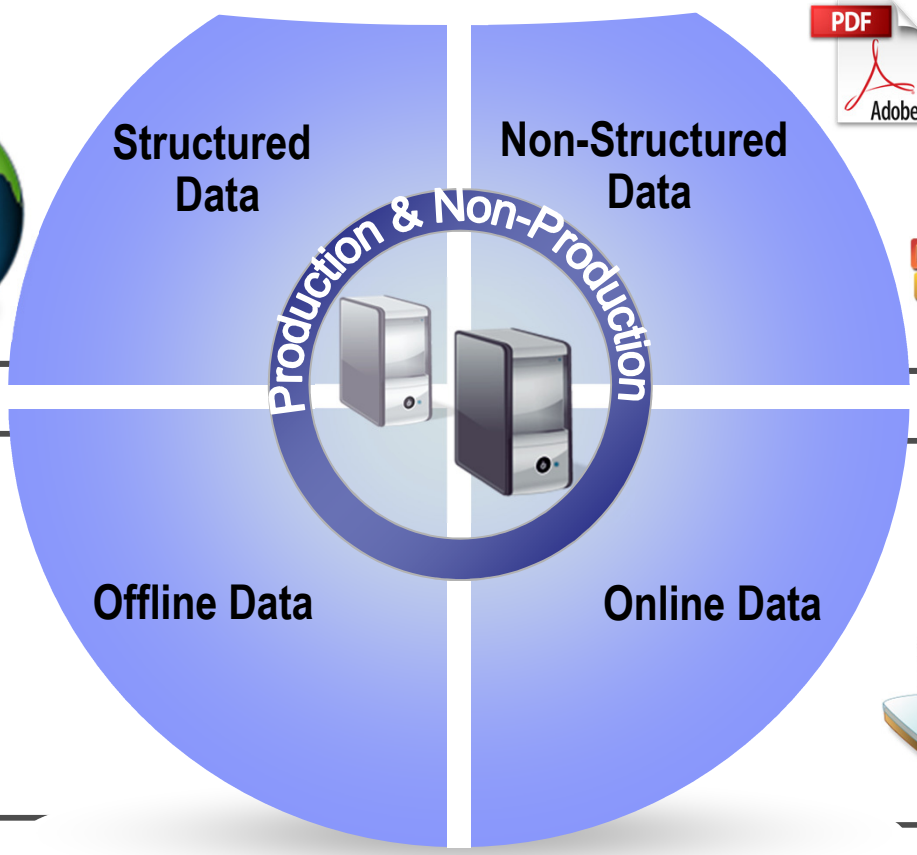
- Activity Monitoring
- VA Assessment
- Masking
- Encryption

Non DB Data

(File Shares, ex. SharePoint, .TIF, .PDF, .doc, scanned documents)

- Data Redaction
- Monitoring file shares

Microsoft Office SharePoint



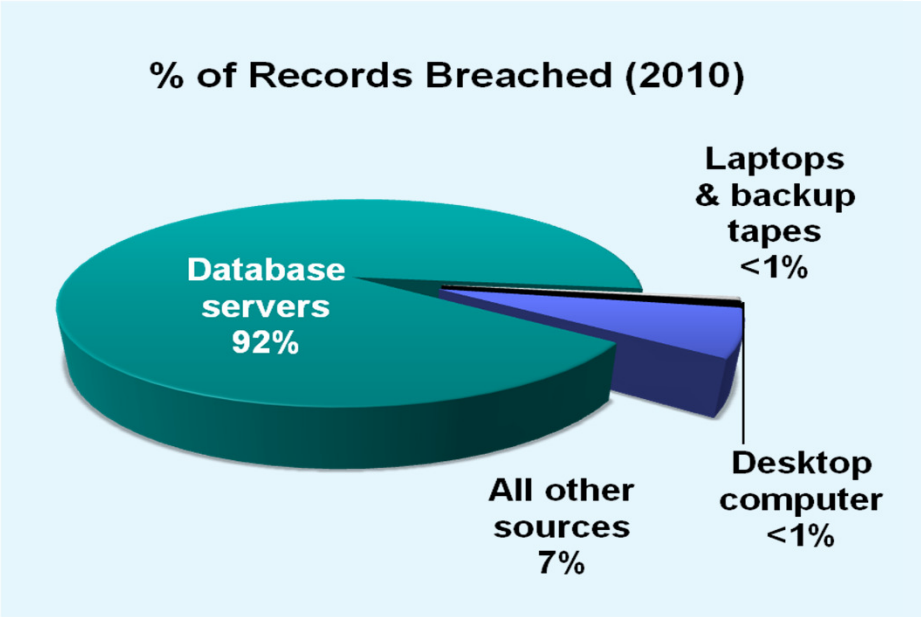
DB Extracted Data

- Encryption
- Masking

Frequently accessed Data

- Activity Monitoring
- VA Test
- Masking
- Encryption

94% of breaches involved database servers in 2012



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

"Go where the money is… and go there often." - Willie Sutton

2010 Data Breach Report from Verizon Business RISK Team
http://www.verizonbusiness.com/resources/security/reports/2010_databreach_rp.pdf

Data Governance goals

1 Prevent data breaches

- Mitigate external and internal threats

2 Ensure the integrity of sensitive data

– Prevent unauthorized changes to data, data infrastructure, configuration files and logs

3 Reduce cost of compliance

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

Common Challenges around Database Security

- How can we monitor user access and detect anomalies?
- How can we control privileged users with direct access?
- Can we store these audit logs in a secure repository?
- Can we have one central audit repository for all database types including Oracle, SQL Server, DB2 and more?
- How can we do all of this with minimal impact to our database and infrastructure?

Addressing Key Stakeholders

SECURITY OPERATIONS

- ✓ Real-time policies
- ✓ Secure audit trail
- ✓ Data mining & forensics

COMPLIANCE AUDIT

- ✓ Separation of duties
- ✓ Best practices reports
- ✓ Automated controls

APPLICATION & DATABASE

- ✓ Minimal impact
- ✓ Change management
- ✓ Performance optimization

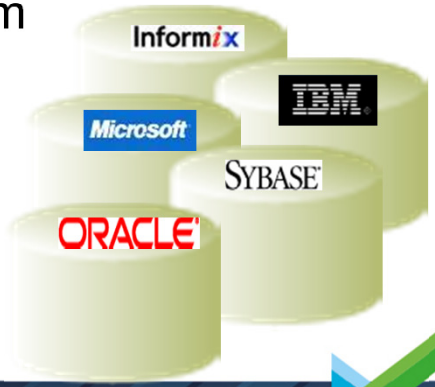
100% Visibility & Unified View

Why Enterprises are Dissatisfied with Traditional Approach

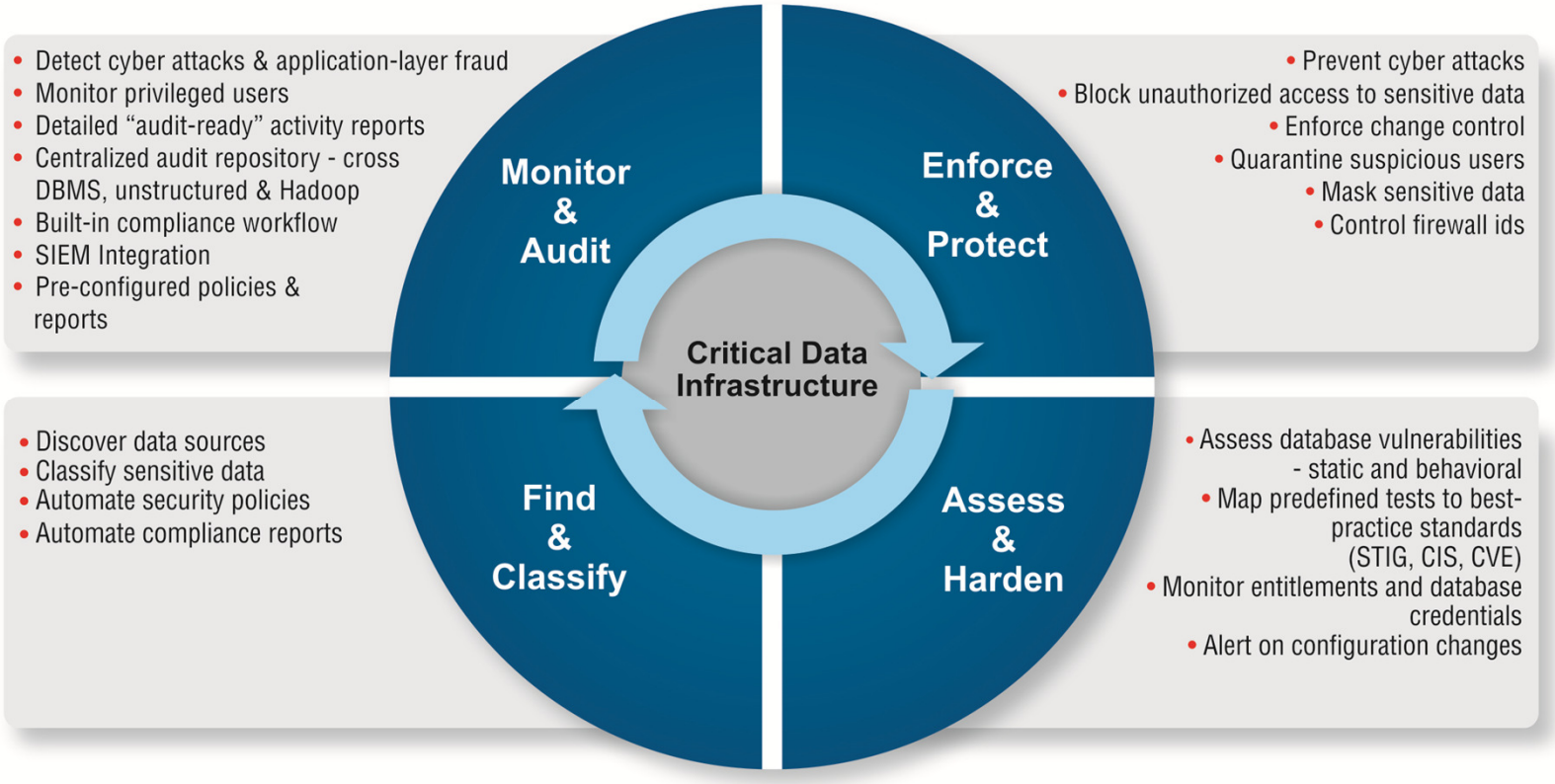
× **Inefficient and costly**
- Database performance is impacted
- Manual processes require valuable resources

× **Provide little value to the business**
- Logs are complicated to inspect
- Any detection is not real-time

× **No segregation of duties**
- Privileged users can bypass the system
- Audit trail can be modified



Addressing the full database security lifecycle

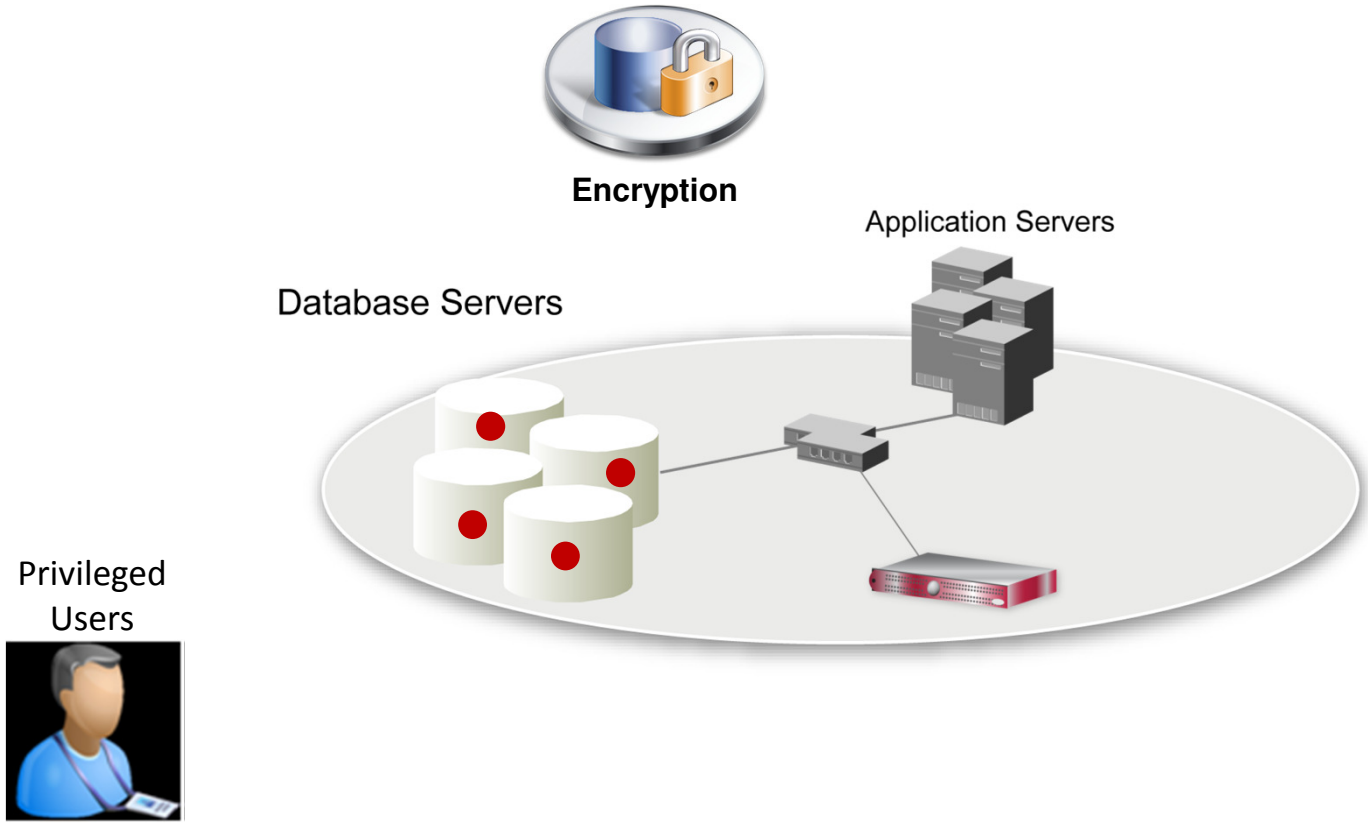


1 Discover
- Discover databases on the network
- Discover where sensitive data is located

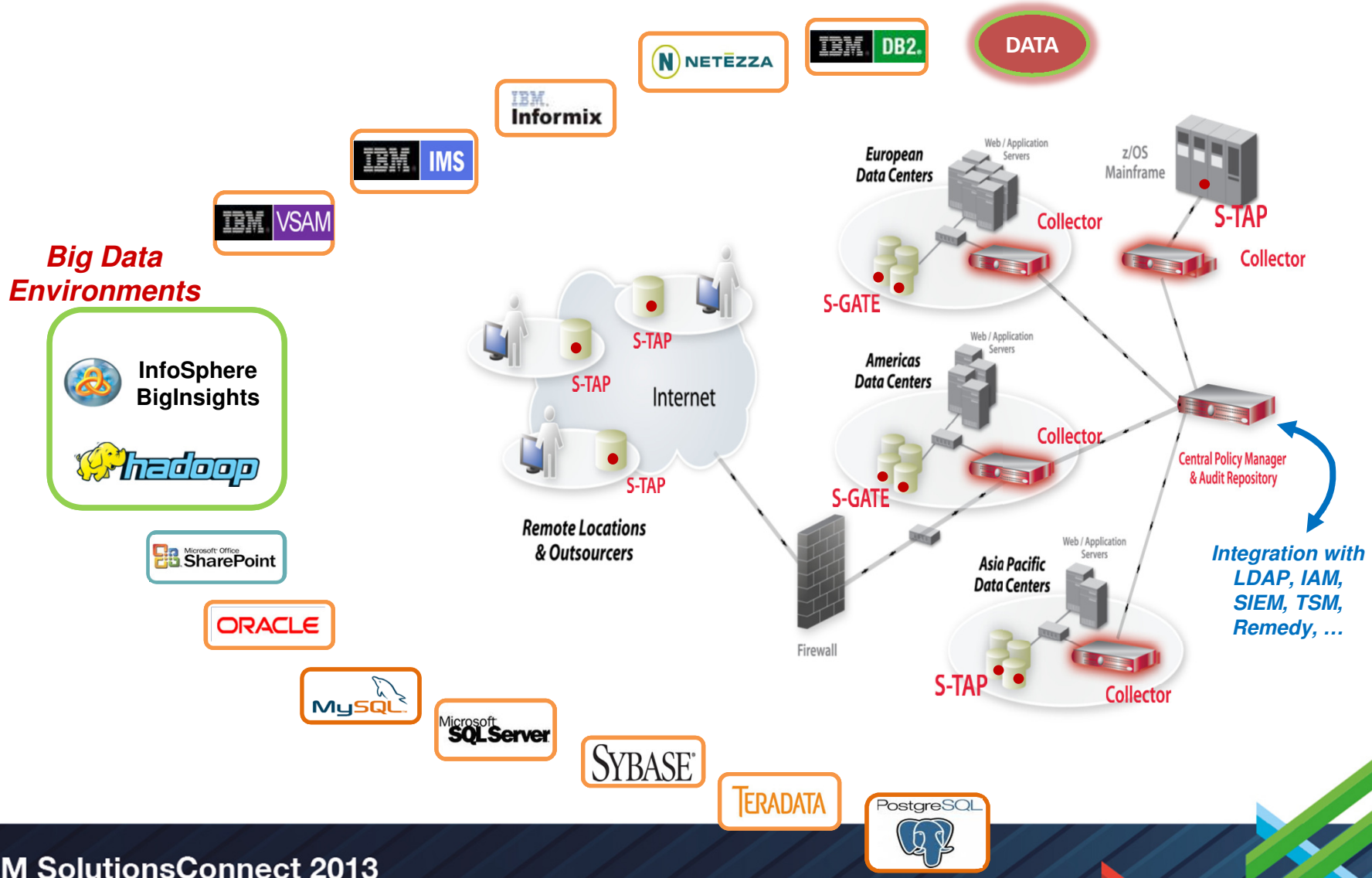
2 Identify Risk
- Perform an assessment to understand risk
- Harden the database to eliminate unnecessary risk

3 Comply
- Monitor database activity to verify security controls
- Automate reporting for proper evidence in compliance process

InfoSphere Guardium: Non-Invasive, Real-Time Security & Audit

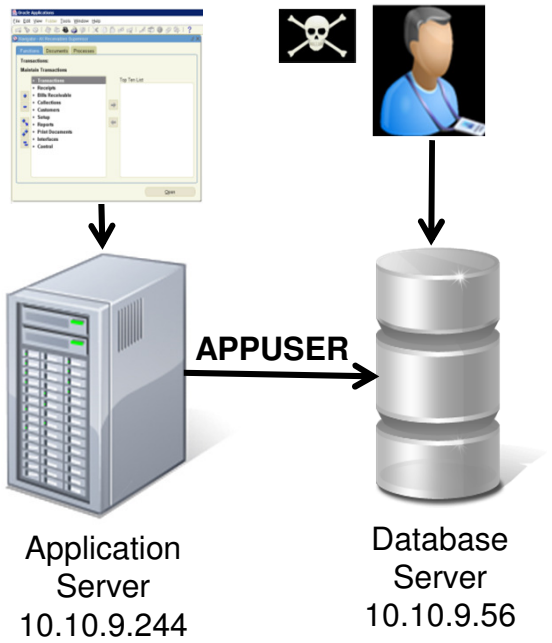


Data warehouses, Big Data, file shares...



Functionalities

Granular Policies with Detective & Preventive Controls



Rule #1 Description: non-App Source AppUser Connection

Category: Security | Classification: Breach | Severity: MED

Not ☐ Server IP / and/or Group: Production Servers

Not ☑ Client IP / and/or Group: Authorized Client IPs

Not ☐ Client MAC | Net. Protocol | and/or Group

Not ☐ DB Name

Not ☐ DB User: APPUSER

Field Name

Object: INVENTORY

Command: DROP TABLE

Min. Ct. 0 | Reset Interval (minutes) 0

Continue to next Rule ☐ | Rec. Vals. ☑

Action: ALERT PER MATCH

Notification

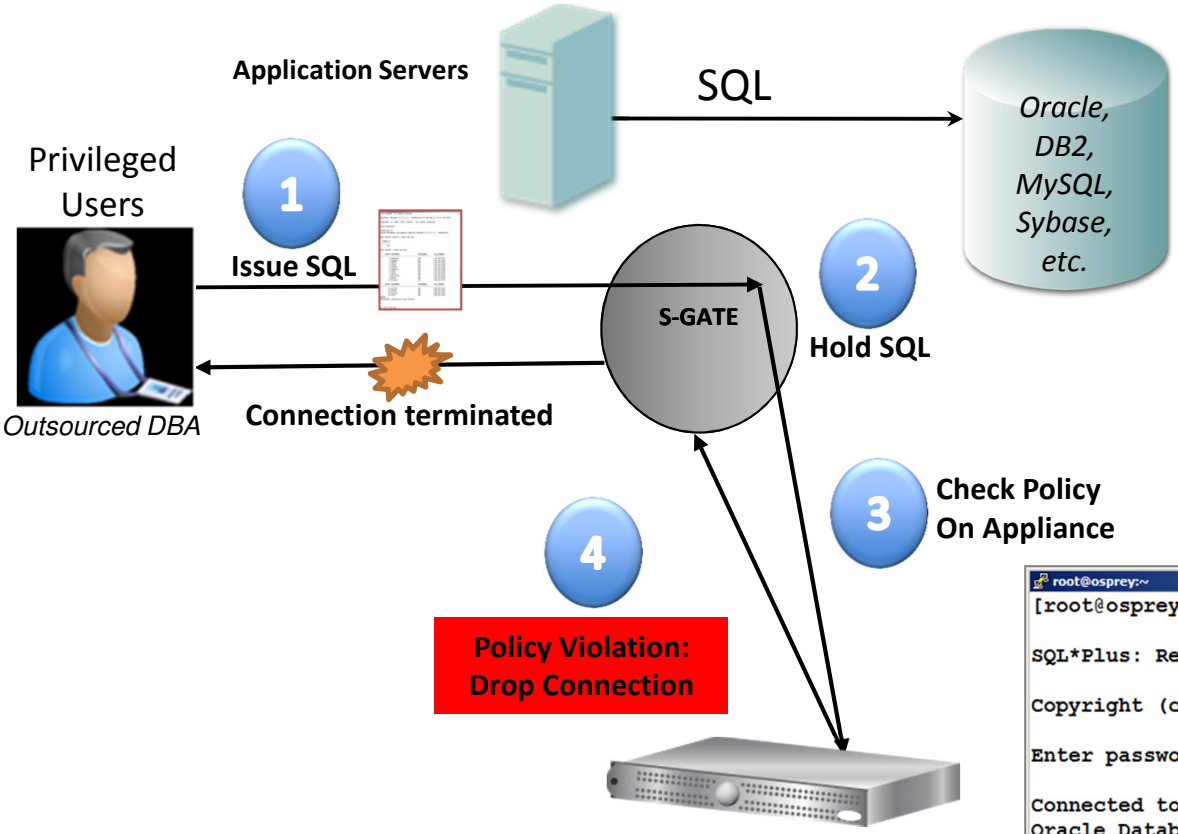
☒ Notification Type MAIL Mail User marc_gamache@guardium.com

ALERT DAILY
ALERT ONCE PER SESSION
ALERT PER MATCH
ALERT PER TIME GRANULARITY
ALLOW
IGNORE RESPONSES PER SESSION
IGNORE SESSION
IGNORE SQL PER SESSION
LOG FULL DETAILS
LOG FULL DETAILS PER SESSION
LOG FULL DETAILS WITH VALUES
LOG FULL DETAILS WITH VALUES PER SESSION
LOG MASKED DETAILS
LOG ONLY
RESET
S-GATE ATTACH
S-GATE DETACH
S-GATE TERMINATE
S-TAP TERMINATE
SKIP LOGGING

From: GuardiumAlert@guardium.com | Sent: Wed 4/15/2009 8:00 AM
To: Marc Gamache
Cc:
Subject: (c1) SQLGUARD ALERT

Subject: (c1) SQLGUARD ALERT Alert based on rule ID non-App Source AppUser Connection
Category: security Classification: Breach Severity MED
Rule # 20267 [non-App Source AppUser Connection]
Request Info: [Session start: 2009-04-15 06:59:03 Server Type: ORACLE Client IP 192.168.20.160 ServerIP: 172.16.2.152 Client PORT: 11787 Server Port: 1521 Net Protocol: TCP DB Protocol: TNS DB Protocol Version: 3.8 DB User: APPUSER
Application User Name
Source Program: JDBC THIN CLIENT Authorization Code: 1 Request Type: SQL_LANG Last Error:
SQL: select * from EmployeeTable

Cross-DBMS, Data-Level Access Control (S-GATE)

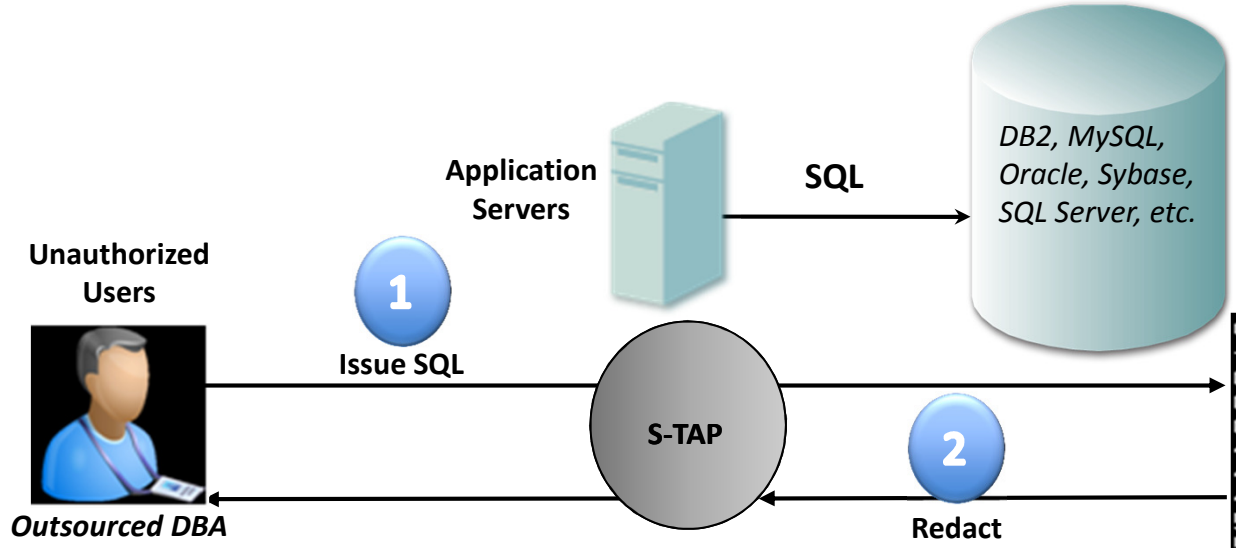


- ✓ Cross-DBMS policies
- ✓ Block privileged user actions
- ✓ No database changes
- ✓ No application changes
- ✓ Without risk of inline appliances that can interfere with application traffic

```
root@osprey:~
[root@osprey ~]# sqlplus system

SQL*Plus: Release 10.2.0.1.0 - Production on Tue May 27 01:13:32 20

Copyright (c) 1982, 2005, Oracle.  All rights reserved.

Enter password:

Connected to:
Oracle Database 10g Express Edition Release 10.2.0.1.0 - Production

SQL> select * from creditcard;
select * from creditcard
*
ERROR at line 1:
ORA-03113: end-of-file on communication channel

SQL>
```

Session Terminated

Protect Stored Data: need to know only



- ✓ Cross-DBMS policies
- ✓ Mask sensitive data
- ✓ No database changes
- ✓ No application changes

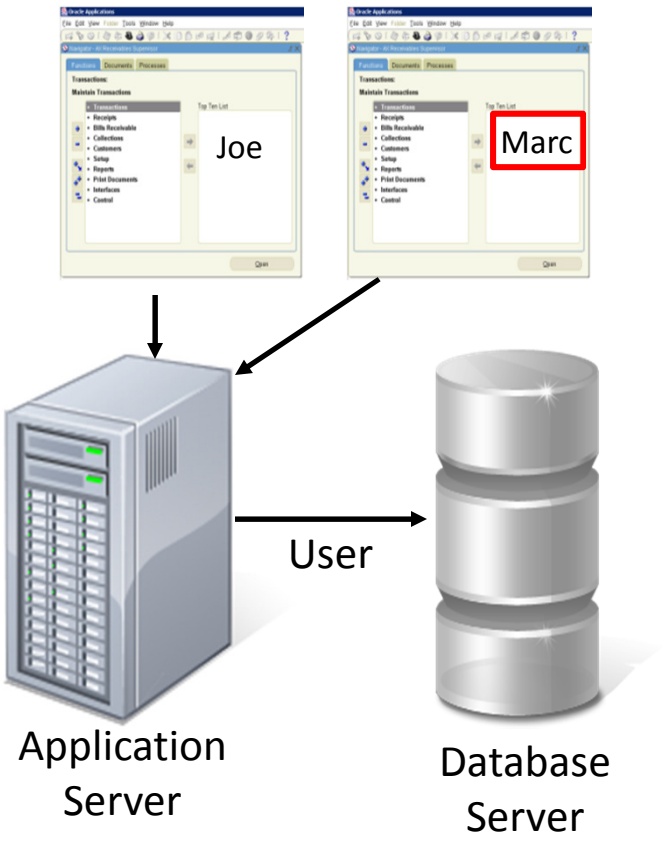
```
CardNumber
-----------------
6011884338876676
6011516565028858
6011839713359946
4486742167789074
4024007126765006
4929493703238250
5175277228903029
5493024612846124
5282335629164185
```

Actual data stored in the database

```
C:\Documents and Settings\Administrator>cqlsh
1> select FirstName, LastName, CardNumber, Pin, SecurityCode from financial.creditcard.CreditCard
2> go
FirstName       LastName                CardNumber                  Pin    SecurityCode
--------------- ----------------------- --------------------------- ----- ------------
Joe             Anthony                 ********** 876676          ***** **30
Joe             Thomas                  ********** 028858          ***** **31
Joe             Smith                   ********** 359946          ***** **32
Joe             Jones                   ********** 789074          ***** **33
Joe             Craven                  ********** 765006          ***** **34
Joe             Shapiro                 ********** 238250          ***** **35
Joe             King                    ********** 903029          ***** **36
Joe             Lynch                   ********** 846124          ***** **37
Joe             Williams                ********** 164185          ***** **38
Joe             Davis                   ********** 87886           ***** **39
Joe             Wilson                  ********** 99418           ***** **10
Joe             Miller                  ********** 96916           ***** **11
Joe             Brown                   ********** 123512          ***** **12
Joe             Dillon                  ********** 123513          ***** **13
Joe             Dole                    ********** 123514          ***** **14
```

Redact and Mask Sensitive Data

Identifying Fraud at the Application Layer



DB User Name	Application User	Sql
APPUSER	joe	select * from EmployeeRoleView where UserName=?
APPUSER	joe	select * from EmployeeTable
APPUSER	marc	insert into EmployeeTable values (?,?,?,?,?,?,?,?)

- ***Issue***: Application server uses generic service account to access DB
  - ***Doesn't identify who*** initiated transaction (connection pooling)
- ***Solution***: Guardium tracks access to application ***user associated with specific SQL commands***
  - Out-of-the-box support for all major enterprise applications (**Oracle EBS, PeopleSoft, SAP, Siebel, Business Objects, Cognos**…) and custom applications **(WebSphere, WebLogic**, ….)
  - Deterministic vs. time-based "best guess"
  - No changes to applications

Vulnerability Assessments Using CIS, STIG Benchmarks

Guardium

Results for Security Assessment: **Comprehensive Oracle Assessment**

Assessment executed 2009-08-21 12:47:28.0

-- Select another result --

From: 2009-08-20 12:47:28.0
To: 2009-08-21 12:47:28.0

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

Download PDF

Tests passing: **42%**

Overall Score

Based on the tests performed under this assessment, data access of the defined database environments requires improvement. Refer to the recommendations of the individual tests to learn how you can address problems within your environment and what you should focus upon first. Once you have begun addressing these problems you should also consider scheduling this assessment as an audit task to continuously assess these environments and track improvement.

View log
Jump to Datasource list

Detailed Scoring

Result Summary *Showing 92 of 92 results (0 filtered)*

	Critical	Major	Minor	Caution	Info
Privilege	9p 15f	-- 1p 4f	-- 1f	-- -- --	-- --
Authentication	2p 4f	-- -- 1f	-- 1f	-- -- --	-- --
Configuration	2p 2f	-- 8p 3f 4e	1p 3f 4e	-- 6f 1e	-- --
Version	-- --	-- -- 2f	-- --	-- -- --	-- --
Other	-- 2f	-- 2p 3f	-- 3p	-- 1e --	-- 6p -- 1e

Current filtering applied:

Severities: - *Show All* -
Scores: - *Show All* -
Types: - *Show All* -

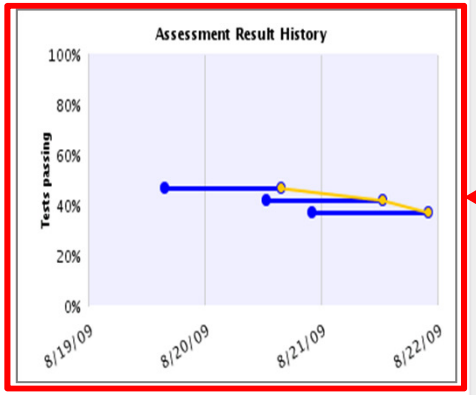
Reset Filtering
Filter / Sort Controls

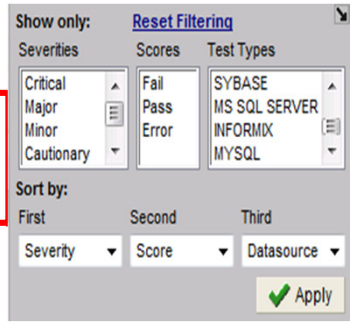
Filter control for easy use

Assessment Test Results Compare with Previous Results *Showing 92 of 92 results (0 filtered)*

Cat.	Test Name	Datasource	P/F	Sev.	Reason
Other	Excessive Login Failures (Production)	[Observed]	Fail	Critical	Too Many login failures, found 15 per day.
					Recommendation: An alarming number of login failures have been reported from your databases. This might be an indication of an attempt to break into your database, or of someone trying to steal or damage your data. The number of login failures should be close to zero, especially in production environments. You should immediately inspect all attempts to access your database and the source of all the login failures, and take immediate action to deny access to your database from unauthorized clients.
Conf.	DBA Profile FAILED_LOGIN_ATTEMPTS Are Limited	ORACLE: oracle - 9.59	Fail	Critical	User profile [MONITORING_PROFILE] setup parameter FAILED_LOGIN_ATTEMPTS found out of defined threshold value

Historical Progress or Regression





Auditing Database Configuration Changes

$ORACLE_HOME/soap/bin/.*	File Pattern	12h	✓	✓
$ORACLE_HOME/sysman/admin/OMSRepositoryConstraints.properties	File Pattern	12h	✓	✓
$ORACLE_HOME/sysman/config/.*properties	File Pattern	12h	✓	✓
$ORACLE_HOME/xdk/admin/xml.properties	File Pattern	12h	✓	✓
ORACLE_BASE	Environment Variable	12h	✓	⊘
ORACLE_HOME	Environment Variable	12h	✓	⊘
ORACLE_SID	Environment Variable	12h	✓	⊘
TNS_ADMIN	Environment Variable	12h	✓	⊘
select * from dba_db_links	SQL Script	12h	✓	⊘

- Tracks changes to files, environment variables, registry settings, scripts, etc.
- 200+ pre-configured templates for all major OS/DBMS configurations
  - Easily customizable via scripts, SQL, etc. (ad hoc tests)
  - Also checks OS permissions for Vulnerability Assessment (VA) tests

Monitoring Data Leakage from High-Value Databases

Should my customer service rep view 99 records in an hour?

Is this normal?

DB User Name	Sql	Records
STEVE	select * from ar.creditcard where i>? and i<?	4
HARRY	select * from ar.creditcard where i<?	4
JOE	select * from ar.creditcard where i<?	99

What exactly did Joe see?

HARRY	select * from ar.creditcard where i<?	**********0002, **********0003, **********0004
JOE	select * from ar.creditcard where i<?	**********0001
JOE	select * from ar.creditcard where i<?	**********0002, **********0003, **********0004, **********0005, **********0006, **********0007, **********0008, **********0009, **********0010, **********0011, **********0012, **********0013, **********0014, **********0015, **********0016
JOE	select * from ar.creditcard where i<?	**********0017, **********0018, **********0019, **********0020, **********0021, **********0022, **********0023, **********0024, **********0025, **********0026, **********0027, **********0028, **********0029, **********0030, **********0031
JOE	select * from ar.creditcard where i<?	**********0032, **********0033, **********0034, **********0035, **********0036, **********0037, **********0038, **********0039, **********0040, **********0041, **********0042, **********0043, **********0044, **********0045, **********0046
JOE	select * from ar.creditcard where i<?	**********0047, **********0048, **********0049, **********0050, **********0051, **********0052, **********0053, **********0054, **********0055, **********0056, **********0057, **********0058, **********0059, **********0060, **********0061
JOE	select * from ar.creditcard where i<?	**********0062, **********0063, **********0064, **********0065, **********0066, **********0067, **********0068, **********0069, **********0070, **********0071, **********0072, **********0073, **********0074, **********0075, **********0076
JOE	select * from ar.creditcard where i<?	**********0077, **********0078, **********0079, **********0080, **********0081, **********0082, **********0083, **********0084, **********0085, **********0086, **********0087, **********0088, **********0089, **********0090, **********0091
JOE	select * from ar.creditcard where i<?	**********0092, **********0093, **********0094, **********0095, **********0096, **********0097, **********0098, **********0099

Tracking Privileged Users Who "su"

Challenge: How do you track users who 'switch' accounts (perhaps to cover their tracks)?

- Native database logging/auditing & SIEM tools can't capture OS user information
- Other database monitoring solutions only provide OS shell account that was used

User activity

```
login as: joe
joe@192.168.30.152's password:
Last login: Tue Apr 14 15:17:12 2009 from 192.168.20.160
[joe@u2 ~]$ su - oracle
Password:
-bash-3.00$ sqlplus system

SQL*Plus: Release 10.2.0.1.0 - Production on Tue Apr 14 15:17:39 2009

Copyright (c) 1982, 2005, Oracle.  All rights reserved.

Enter password:

Connected to:
Oracle Database 10g Express Edition Release 10.2.0.1.0 - Production

SQL> insert into AppUser.EmployeeTable values (1001,6,'Joe','Smith','Salary','Bonus',500000,1);

1 row created.

SQL>
```

What Guardium Shows You

DB User Name	Sql
SYSTEM	insert into AppUser.EmployeeTable values (?,?,?,?,?,?,?,?)

DB User Name	ShellAcct	Sql
SYSTEM	ORACLE	insert into AppUser.EmployeeTable values (?,?,?,?,?,?,?,?)

DB User Name	ShellAcct	OSUser	Sql
SYSTEM	ORACLE	joe	insert into AppUser.EmployeeTable values (?,?,?,?,?,?,?,?)

Protecting Against Vulnerabilities With Virtual Patching

Rule #2 Description: Terminate Access to Vulnerable Objects

Category: Data Security | Classification: Known Vulnerabilities | Severity: HIGH

Not ☐ Server IP / and/or Group: Production Servers

Not ☐ Client IP / and/or Group: ----------

Not ☐ Client MAC | Net. Protocol | and/or Group: ----------

DB Type: ---------- | Not ☐ Service Name | and/or Group: ----------

Not ☐ DB Name | and/or Group: ----------

Not ☑ DB User | and/or Group: (Public) Authorized Users

Not ☐ App. User | and/or Group: ----------

Not ☐ OS User | and/or Group: ----------

Not ☐ Src App. | and/or Group: ----------

Not ☐ Field Name | and/or Group: ----------

Not ☐ Object | and/or Group: (Public) Vulnerable Objects (with wildcards)

Not ☐ Command | and/or Group: ----------

Object/Command Group: ----------

Object/Field Group: ----------

Pattern | XML Pattern

Period: ----------

App Event Exists ☐ | Event Type | Event User Name

App Event Values

Text | Numeric | Date

Min. Ct. 0 | Reset Interval (minutes) 0

Continue to next Rule ☐ | Rec. V... ☐

Action: S-GATE TERMINATE

Cancel | Comment | Accept

Group Members:

%BFILENAME.%
%BUMP_SEQUENCE.%
%CANONICALIZE.%
%CDC_DROP_CTABLE_BEFORE.%
%CHANGE_TABLE_TRIGGER.%
%CHECK_DDL_TEXT.%
%CHGTAB_CACHE.%
%COMPRESSDATA.%

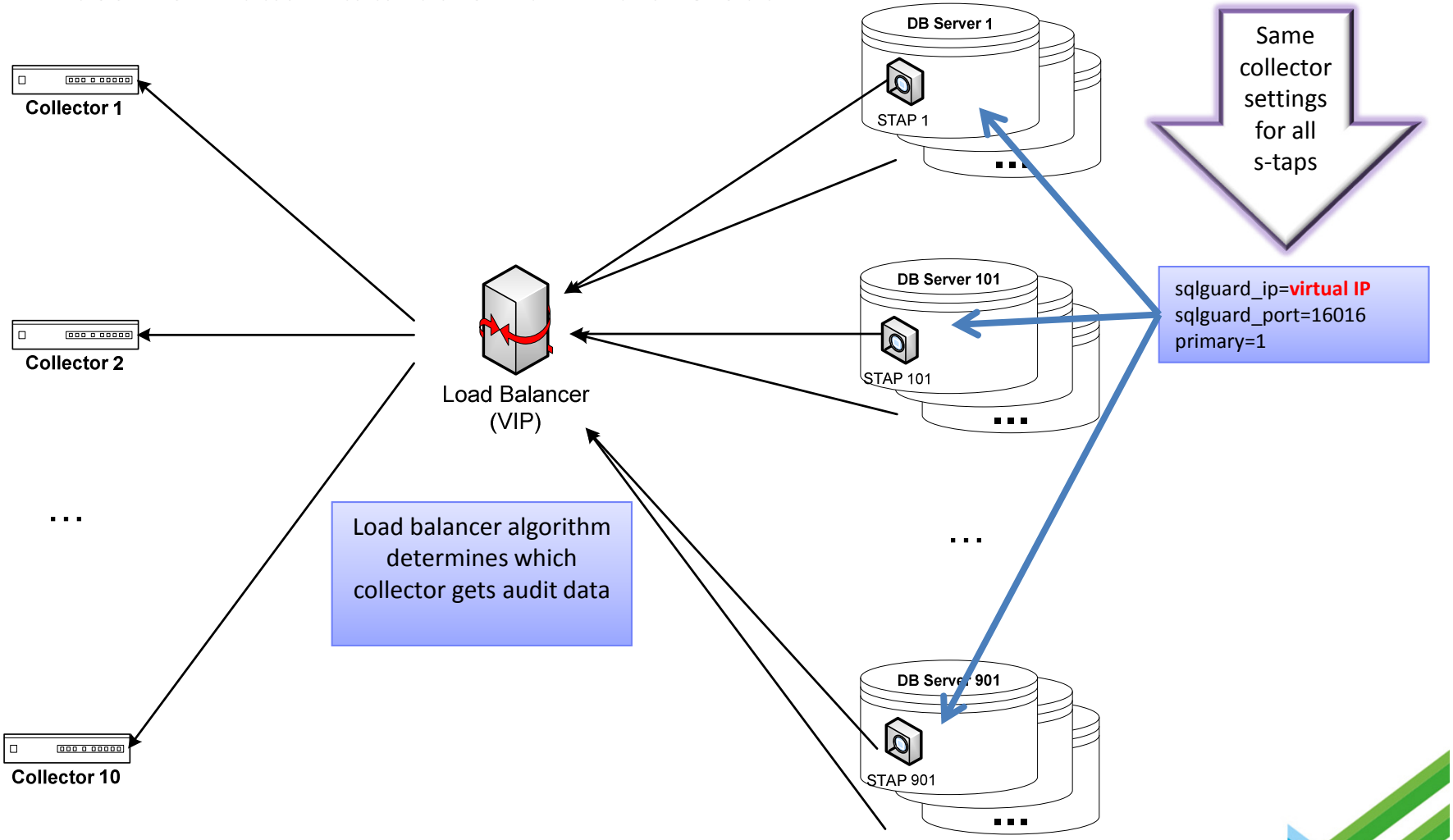
Vulnerable procedure that can't be patched right away

What the user sees

```
[root@ora-vm1 va-notes]# sqlplus joe

SQL*Plus: Release 10.2.0.1.0 - Production on Fri Aug 21 23:37:50 2009

Copyright (c) 1982, 2005, Oracle.  All rights reserved.

Enter password:

Connected to:
Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 - Production
With the Partitioning, OLAP and Data Mining options

SQL> @bump_sequence.sql
DECLARE
*
ERROR at line 1:
ORA-03113: end-of-file on communication channel

SQL> select * from all_users;
ERROR:
ORA-03114: not connected to ORACLE

SQL>
```

Guardium Grid: Load Balancing / High Availability

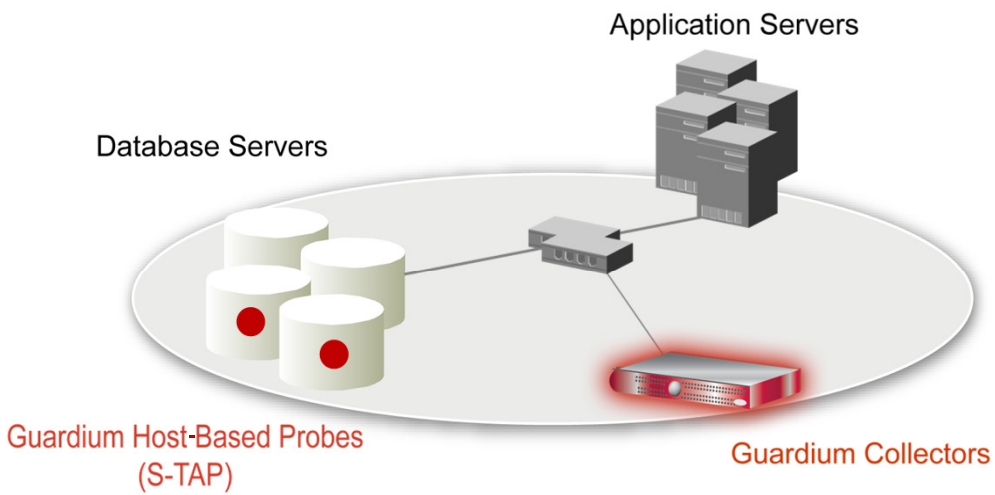
Test with Load Balancers from F5 & Cisco



SOX & PCI Compliance for Major Retailer

- **Who:** National retailer with >$50B in sales & 6,400 stores
- **Need:** Initially PCI, then extended to SOX, SAS70, data privacy
- **Environment:** 5 major data centers
  - Oracle, SQL Server, DB2, UDB on AIX, Solaris, Windows
  - PeopleSoft & SAP plus custom applications
- **Alternatives Considered:**
  - Native database auditing
  - Database encryption
  - Database security appliance from major security vendor
- **Results**
  - Implemented in ~ 4 weeks
  - PCI certified in stipulated time, saving millions in potential penalties
  - Compensating control for DB encryption (Requirement 3.4)
  - Requirement 6: Maintain secure systems (enforce change controls)
  - Automated solution for Requirement 10 (Track & monitor all access to cardholder data)
  - Side-benefits
    - Application performance optimized by identifying issue with failed DB calls
    - Load distribution optimized between servers

Summary



- Continuously monitors **<u>all</u> database activities** (local/network access)
- Heterogeneous, cross-DBMS solution
- Does not rely on native DBMS logs
- Minimal performance impact (2-3%)
- No DBMS or application changes
- Activity logs can't be erased by attackers or DBAs
- Automated compliance reporting, sign-offs & escalations (SOX, PCI, NIST, etc.)
- Dynamic DrillDown reporting for **forensic**
  - ***Who, what, when, where, how***