



## Agenda

- Business drivers for database security
- InfoSphere Guardium architecture
- Common applications
- The InfoSphere portfolio
- Case studies

## Database Activity Monitoring: Three Key Business Drivers

### 1. Prevent data breaches

- Mitigate external and internal threats



### 2. Ensure data integrity

- Prevent unauthorized changes to sensitive data



### 3. Reduce cost of compliance

- Automate and centralize controls

Across DBMS platforms and applications

Across SOX, PCI, SAS70, ...

- Simplify Processes
- Reduce Cost



Provide insight such as . . .

- **Who** is changing database schemas or dropping tables?
- **When** are there any unauthorized source programs changing data?
- **What** are DBAs or outsourced staff doing to the databases?
- **How** many failed login attempts have occurred?
- **Who** is extracting credit card data?
- **What** data is being accessed from which network node?
- **What** data is being accessed by which application?
- **How** is data being accessed?
- **What** are the access patterns based on time of day?
- **What** database errors are being generated?
- **What** is the exposure to sensitive objects?
- **When** is someone attempting an SQL injection attack?



## Database Security Pain Points

- Protecting sensitive enterprise data, typically distributed across a large number of servers and a variety of DBMS platforms, from unauthorized access, theft or changes
- Successfully passing a growing variety of audits (to validate compliance with SOX, PCI DSS, data privacy and other regulatory mandates as well as internal governance controls)
- Reducing the cost of compliance activities, which typically involve resource intensive and error-prone manual controls
- Manually reading through database logs
- Dealing with the performance degradation resulting from turning on native database auditing

## Key Questions

- Have you experienced any database breaches?
- What processes do you have in place to protect high-value enterprise information?
- Are you facing challenges in complying with PCI DSS, SOX, data privacy or other regulatory mandates?
- Are your costs increasing due to the resources required to support audit and compliance activities
- Are you concerned with internal threats to your sensitive data?
- Do you have database or application performance issues resulting from the use of native database logging to support compliance activities?
- Do you always have a view of what changes are occurring in your database and who is accessing what data? How are you alerted to activities out of the ordinary?

## The Compliance Mandate

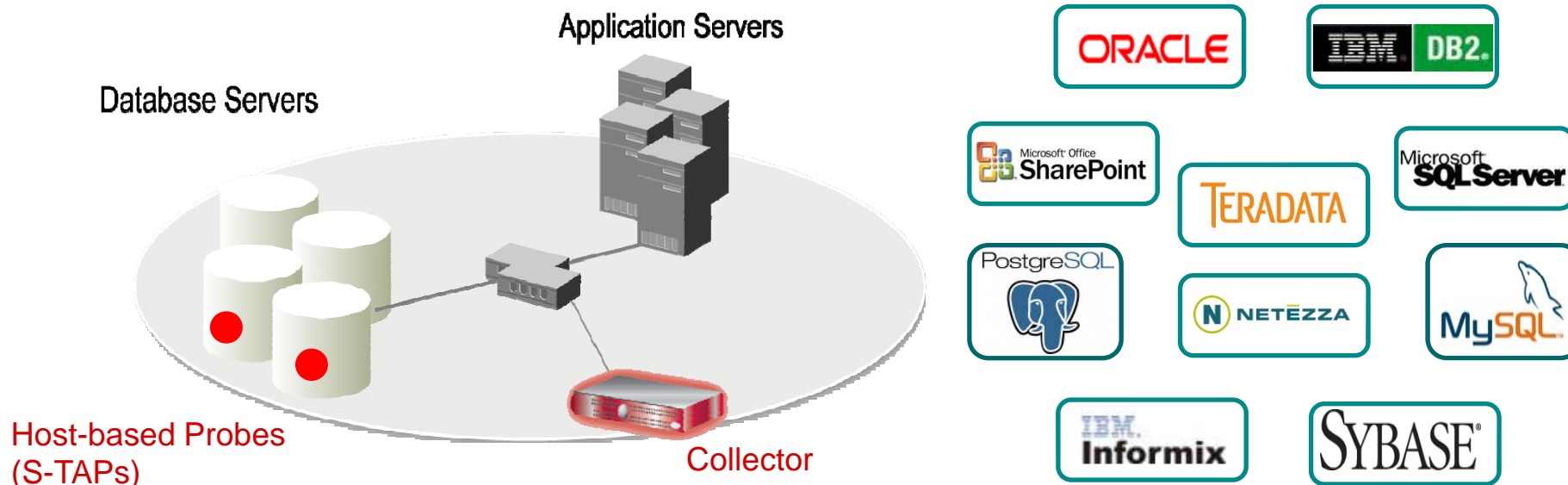
Audit Requirements	COBIT (SOX)	PCI-DSS	ISO 27002	Data Privacy & Protection Laws	NIST SP 800-53 (FISMA)
1. Access to Sensitive Data (Successful/Failed SELECTs)		✓	✓	✓	✓
2. Schema Changes (DDL) (Create/Drop/Alter Tables, etc.)	✓	✓	✓	✓	✓
3. Data Changes (DML) (Insert, Update, Delete)	✓		✓		
4. Security Exceptions (Failed logins, SQL errors, etc.)	✓	✓	✓	✓	✓
5. Accounts, Roles & Permissions (DCL) (GRANT, REVOKE)	✓	✓	✓	✓	✓

**DDL = Data Definition Language (aka schema changes)**

**DML = Data Manipulation Language (data value changes)**

**DCL = Data Control Language**

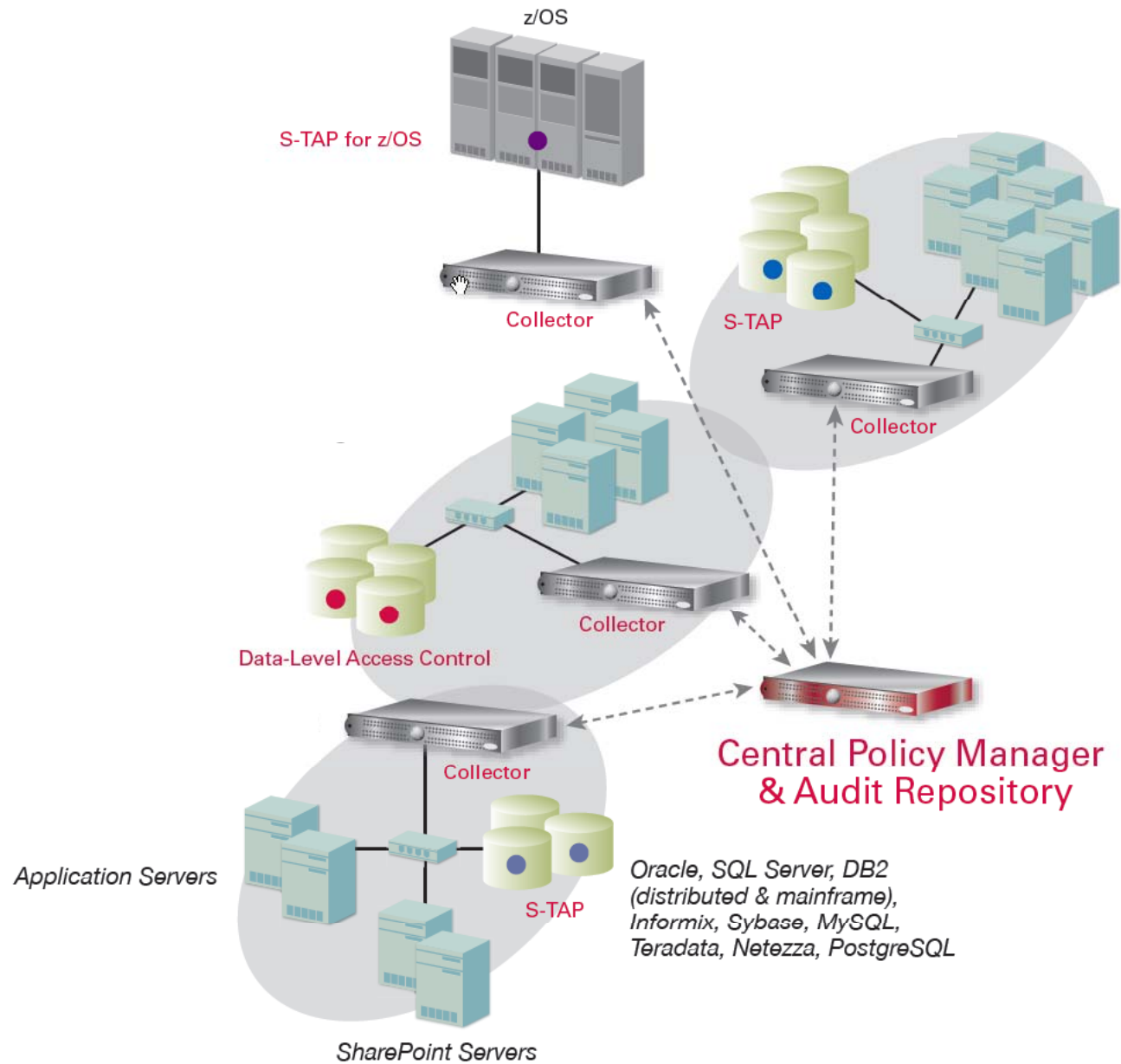
## Real-Time Database Monitoring with InfoSphere Guardium



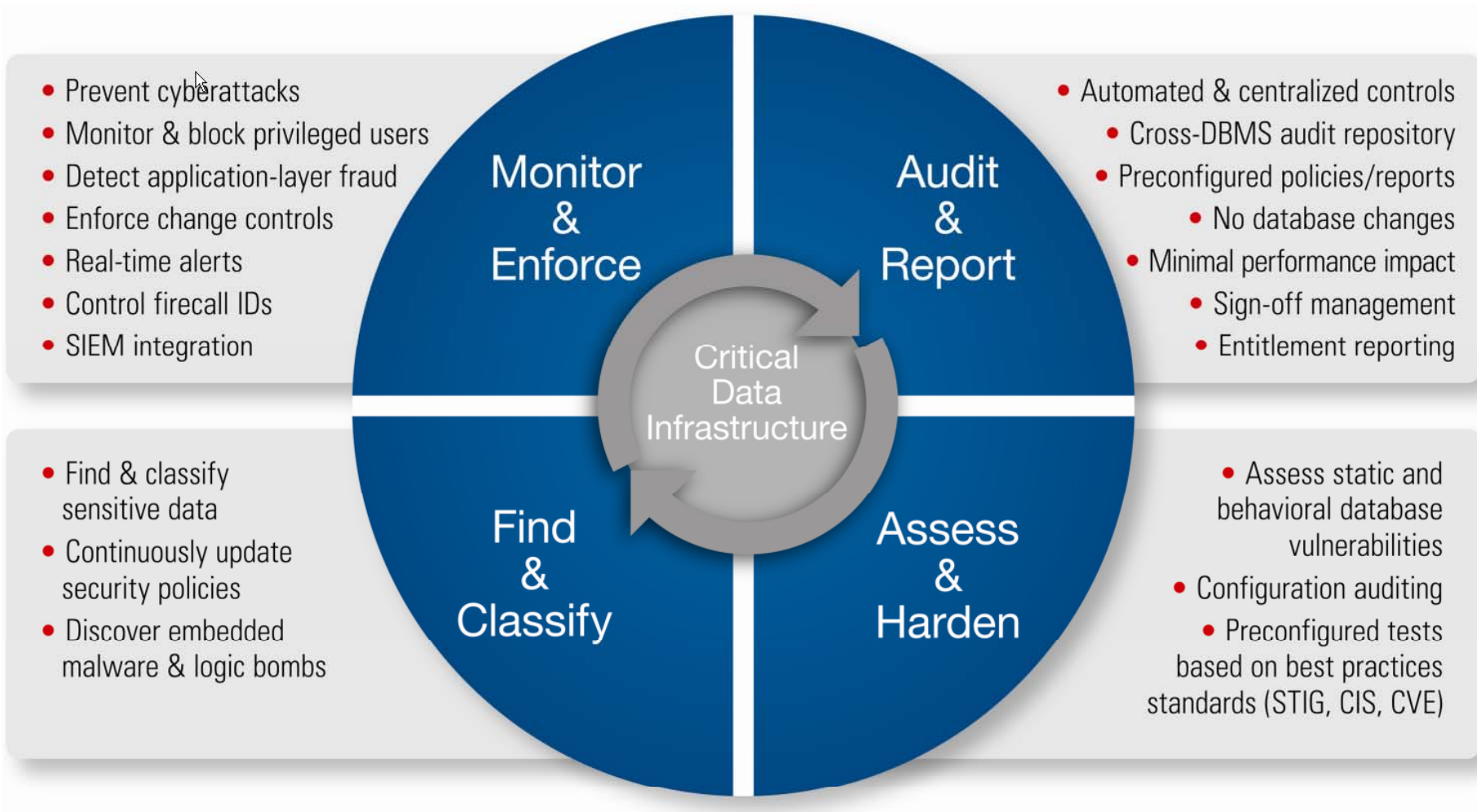
- Non-invasive architecture
  - Outside database
  - Minimal performance impact
  - No DBMS or application changes
- Cross-DBMS solution
- 100% visibility including local DBA access
- Enforces separation of duties
- Does not rely on DBMS-resident logs that can easily be erased by attackers, rogue insiders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



# Scalable Multi-Tier Architecture



## Addressing the Complete Database Security and Compliance Lifecycle



# Discover Sensitive Data

## Find Cardholder Data

### Databases Discovered

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

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

### Classification Rule #1 For Classification Policy "find creditcard data"

Rule Name: Send Alert

Category: PCI

Internet Explorer provided by

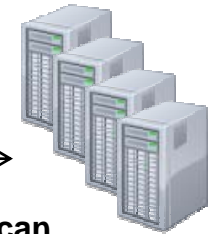
Certificate Error

Catalog	Schema	Table Name	Column Name	Rule Description	Comments	Classification Name	Category	Data Source Description
	HR	BINSRfXc0W/34qTgQAoKNwkbuw==50	CARDNUMBER	Send Alert	Date: Monday, July 21, 2008 6:30:22 PM EDT Datasource: ORACLE 10.10.9.56:1521 xe Object: TABLE HR.BINSRfXc0W/34qTgQAoKNwkbuw==50 VARCHAR2(30) CARDNUMBER Category: 'PCI' Classification: 'Cardholder Data' Rule: Search For Data: Send Alert TABLE_TYPE='TABLE,VIEW', DATA_TYPE='TEXT', SEARCH_VALUE_PATTERN='[0-9]{4}-[0-9]{4}-[0-9]{4}-[0-9]{4}' Action: Send Alert: Send Alert Urgent Flag='false', Receiver='SYSLOG' Action: Log Policy Violation: Send Policy Violation Severity='10' Action: Add To Group Of Objects: add to group Object Group='PCI Cardholder Sensitive objects', Replace Group Content='false'	Cardholder Data	PCI	10-56-sy



Guardium

Agentless Network Scan  
10.10.9.\*



Search Like: [ ]

Search Expression: `[0-9]{4}-[0-9]{4}-[0-9]{4}-[0-9]{4}` [RE]

Maximum Rows: [ ]

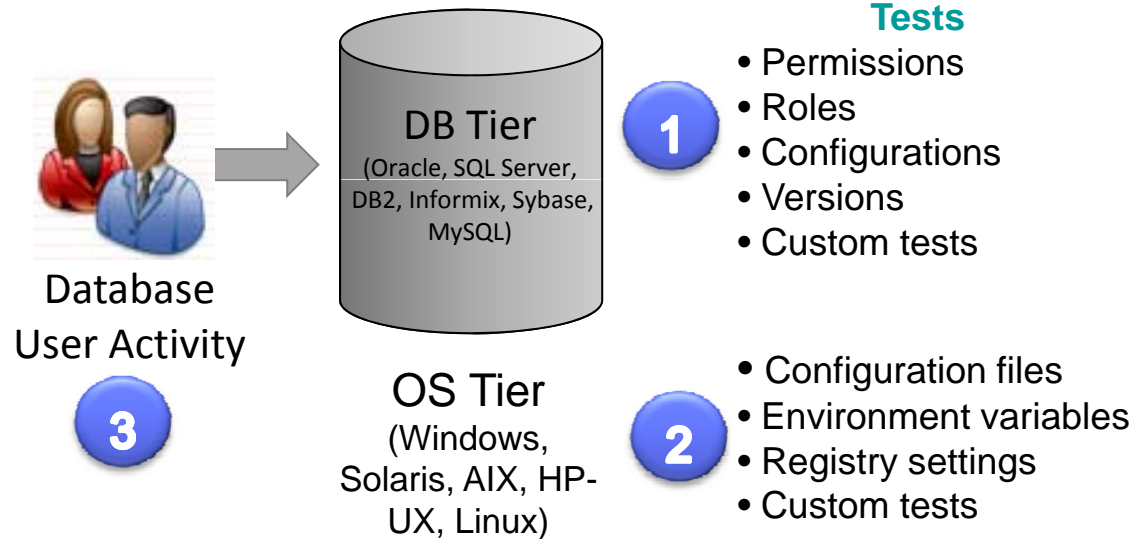
Classification Rule Actions: + New Action

- 1 Send Alert (Send Alert)
- 2 Send Policy Violation (Log Policy Violation)
- 3 add to group (Add To Group Of Objects)

Cancel Accept

## Vulnerability & Configuration Assessment Architecture

- Based on industry standards (DISA STIG & CIS Benchmark)
- Customizable
  - Via custom scripts, SQL queries, environment variables, etc.
- Combination of tests ensures comprehensive coverage:
  - Database settings
  - Operating system
  - Observed behavior



# Vulnerability Assessment Example

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

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

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](#)

**Overall Score**

Tests passing: **42%**

**Assessment Result History**

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 Matrix**

**Filter control for easy use**

**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](#)

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

Cat.	Test Name	Datasource	P/F	Sev.	Reason
Other	<a href="#">Excessive Login Failures (Production)</a>	[Observed]	Fail	Critical	Too Many login failures, found 15 per day.  <i>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.</i>
Conf.	<a href="#">DBA Profile FAILED_LOGIN_ATTEMPTS Are Limited</a>	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

Show only: [Reset Filtering](#)

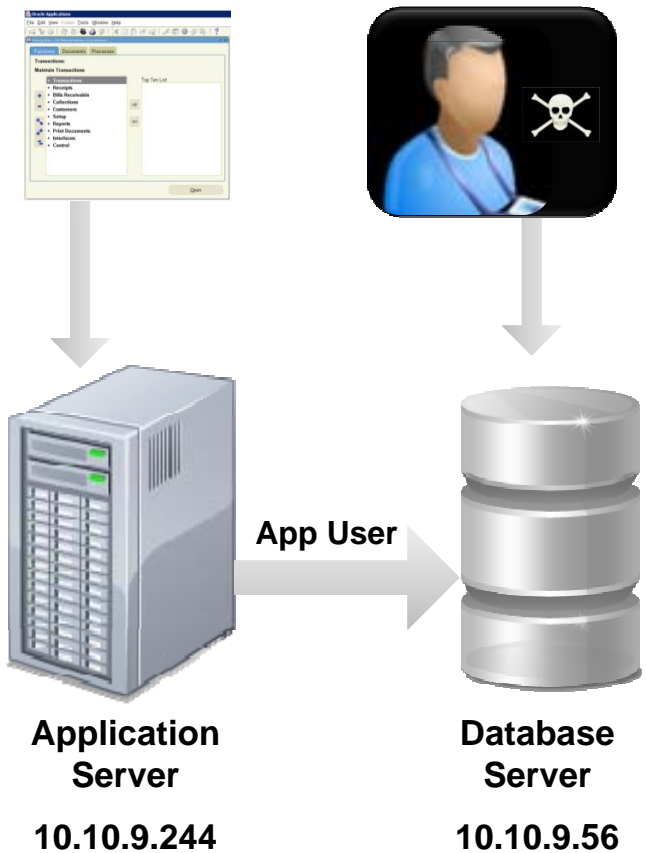
Severities	Scores	Test Types
Critical	Fail	SYBASE
Major	Pass	MS SQL SERVER
Minor	Error	INFORMIX
Cautionary		MYSQL

Sort by:

First	Second	Third
Severity	Score	Datasource

Apply

# Granular Policies with Real-Time Alerts



**Rule #1 Description** non-App Source AppUser Connection

**Category** Security **Classification** Breach **Severity** MED

**Hot**  **Server IP** / and/or Group Production Servers

**Hot**  **Client IP** / and/or Group Authorized Client IPs

**Hot**  **Client MAC** and/or Group

**DB Type** and/or Group **Hot**  **Service Name** and/or Group

**Hot**  **DB Name** and/or Group

**Hot**  **DB User** APPUSER and/or Group

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

**Continue to next Rule**  **Rec. Vals.**

**Action** ALERT PER MATCH

**Notification**

**Notification Type** MAIL **Mail User** marc

From: GuardumAlert@guardum.com  
 To: Marc Gamache  
 Cc:  
 Subject: (c1) SQLGUARD ALERT

Sent: Wed 4/15/2009 8:00 AM

Subject: (c1) SQLGUARD ALERT Alert based on rule 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

**Alert** on any login using the application account sourced from a location other than the application!

# Cross-DBMS Policies and Auditing

**Access Rule Definition** ?

Rule #2 of policy v8

Description: Granular Cross Platform Policy Rule

Category: Security    Classification: Operations    Severity: HIGH

Not  Server IP [ ] / [ ] and/or Group: (Public) PCI Authorized Server IPs

Not  Client IP [ ] / [ ] and/or Group: (Public) PCI Authorized Client IPs

Not  Client MAC [ ]

Net Prtcl. [ ] and/or Group: [ ]

DB Type: [ ]

Not  Svc. Name [ ] or Group: [ ]

Not  DB Name [ ] or Group: [ ]

Not  DB User [ ] or Group: [ ]

Client IP/Src [ ]

Not  App. User [ ] or Group: [ ]

Not  OS User [ ] or Group: [ ]

Not  Src App. [ ] or Group: [ ]

Not  Field [ ] or Group: [ ]

Not  Object [ ] or Group: (Public) PCI Cardholder Sensitive objects

Not  Command [ ] and/or Group: [ ]

Object/Cmd. Group: [ ]

Object/Field Group: [ ]

Pattern [ ] RE

XML Pattern [ ] RE

App Event Exists     Event Type [ ]    Event User Name [ ]

App Event Values Text [ ] and/or Group: [ ]

Numeric [ ]    Date [ ]

Data Pattern [ ] RE    Replacement Character \* [ ]

Time Period [ ]

Minimum Count [0]    Reset Interval [0] minutes    Message Template [Default]

Quarantine for [0] minutes    Records Affected Threshold [0]    Rec. Vals.     Cont. to next rule

**Actions**

+ **ALERT PER MATCH**

Add Action

Back    Save

- Single set of cross-DBMS policies
- Single cross-DBMS audit repository for enterprise-wide correlation and reporting

## Capture Audit Data

```

192.168.2.148 - PuTTY
-bash-3.00$ sqlplus system

SQL*Plus: Release 9.2.0.6.0 - Production on Mon Dec 8 12:19:22 2008

Copyright (c) 1982, 2002, Oracle Corporation. All rights reserved.

Enter password:

Connected to:
Oracle9i Enterprise Edition Release 9.2.0.6.0 - 64bit Production
With the Partitioning, OLAP and Oracle Data Mining options
JServer Release 9.2.0.6.0 - Production

SQL> select * from ar_trx_bal_summary;
select * from ar_trx_bal_summary

ORA-03113: end-of-file on communication channel

SQL>
    
```

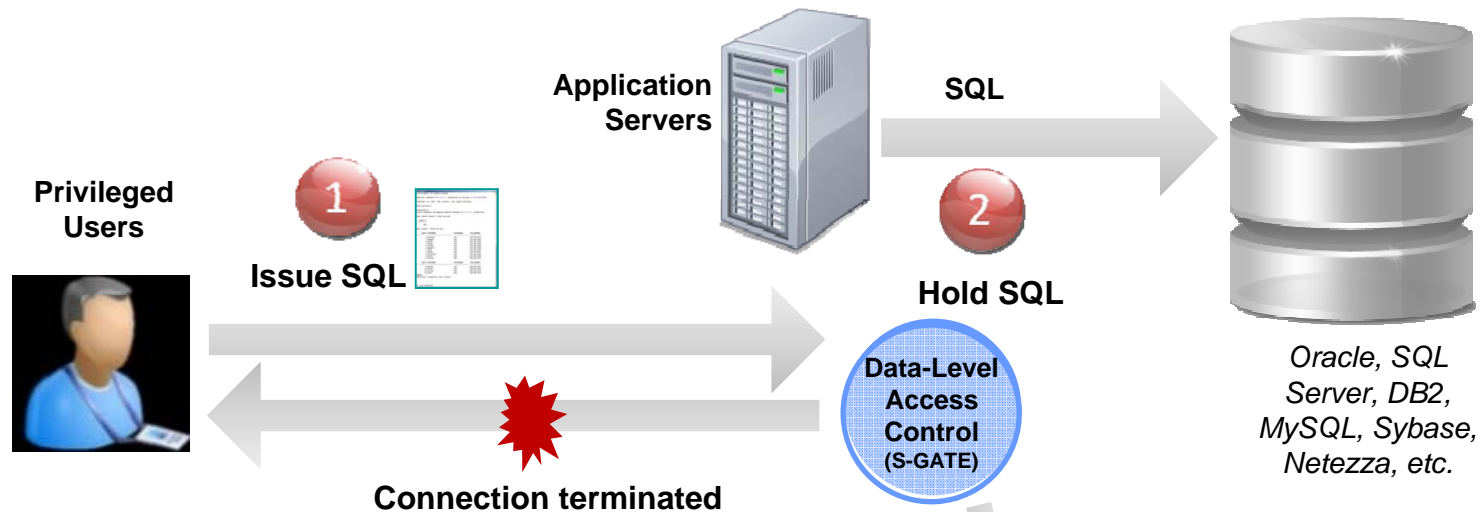
Policy Violations / Incident Management

Start Date: 2008-12-08 10:25:04 End Date: 2008-12-09 11:25:04

Violation Log Id	Timestamp	Category Name	Access Rule Description	Client IP	Server IP	DB User Name	Full SQL String	Severity Description
758	2008-12-08 12:21:46.0	sox	terminate unauthorized user access to EBS	192.168.2.148	192.168.2.148	SYSTEM	select * from ar_trx_bal_summary	HIGH



# Blocking Access Without Inline Appliances



```

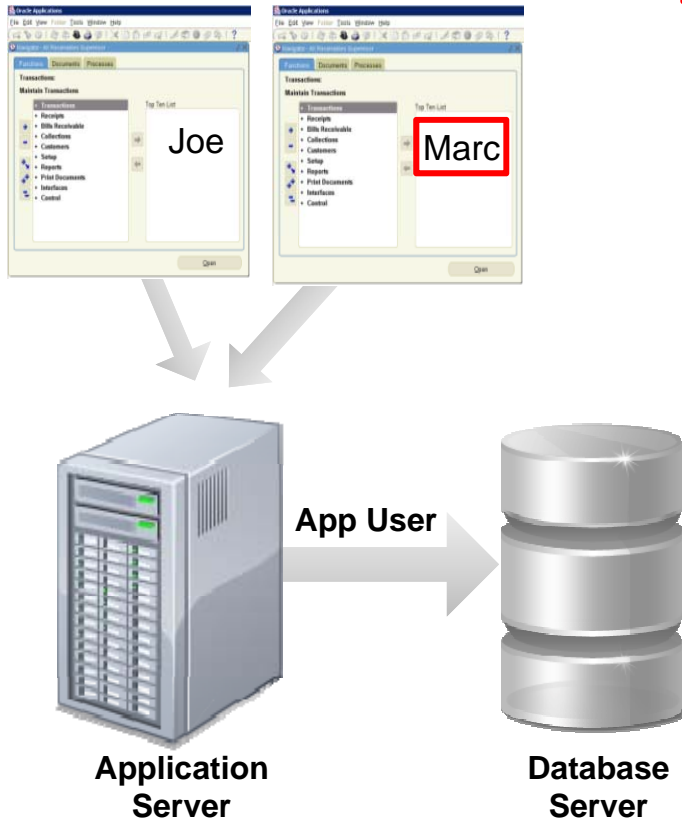
root@osprey:~# sqlplus system
SQL*Plus: Release 10.2.0.1.0 - Production on Tue May 27 01:13:32 20
Copyright (c) 1982, 2005, Oracle. All rights reserved.
Enter password:
Connected to:
Oracle Database 10g Express Edition Release 10.2.0.1.0 - Production
SQL> select * from creditcard;
select * from creditcard
*
ERROR at line 1:
ORA-03113: end-of-file on communication channel
    
```

Session Terminated



# Identifying Fraud in Connection-Pooled Applications

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:** App server uses generic service account to access DB - which doesn't identify WHO initiated transaction (connection pooling)
- **Solution:** Track access to application users associated with specific SQL commands
  - Deterministic identification vs. time-based "best guess"
  - Out-of-the-box support for all major enterprise apps (Oracle EBS, PeopleSoft, SAP, Siebel, Business Objects, Cognos, etc.)
  - Plus custom apps (WebLogic, WebSphere, Oracle AS, etc.)
  - No changes to applications

## Mask Sensitive Information From Unauthorized Users

```

C:\>sqlcmd
1> select * from ssn where ssnid < 5
2> go
SSNID      LastName      FirstName      SSN_Number
-----
0 Anthony      joe            *****-6780
1 Thomas      joe            *****-6781
2 Smith       Joe            *****-6782
3 Jones       Joe            *****-6783
4 Craven      Joe            *****-6784

(5 rows affected)
1> quit

C:\>sqlcmd
1> select * from ssn where ssnid < 5
2> go
SSNID      LastName      FirstName      SSN_Number
-----
0 Anthony      joe            123-45-6780
1 Thomas      joe            123-45-6781
2 Smith       Joe            123-45-6782
3 Jones       Joe            123-45-6783
4 Craven      Joe            123-45-6784

(5 rows affected)
    
```

Masked values to database client

Actual Values in the database server

- Mask data on the fly for production database servers

# Report Builder

Query Builder - Windows Internet Explorer  
 https://10.10.9.248:8443/queryBuilderDirectOpen.do?cmd=querySelected&selectedQuery=Client+IPs+Activity&selectedQueryIndex=302

**Entity List**

- Client/Server
  - 7AX5 Access Id
  - Timestamp
  - Timestamp Date
  - Timestamp Time
  - Timestamp WeekDay
  - Timestamp Year
- Server Type
- 123 Client IP
- 321 Server IP
- Network Protocol
- DB Protocol
- DB Protocol Version
- DB User Name
- Source Program
- 7AX5 Client MAC
- 'hostX' Client Host Name
- svcX Service Name
- Server OS
- Client OS
- OS User
- 'hostX' Server Host Name
- desc: Server Description

**Client IPs Activity**

Main Entity: Object  Add Count  Add Distinct  Sort by count

Query Fields							
	Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
<input type="checkbox"/>	1	Client/Server	Client IP	Value	<input type="checkbox"/>		
<input type="checkbox"/>	2	Command	SQL Verb	Value	<input type="checkbox"/>		
<input type="checkbox"/>	3	Object	Object Name	Value	<input type="checkbox"/>		

Addition mode:  AND  OR  HAVING

Query Conditions							
	Entity	Agg.	Attribute	Operator	Runtime Param.		
<input type="checkbox"/>	WHERE	Command	SQL Verb	LIKE	Parameter	CommandLike	
<input type="checkbox"/>	AND	Object	Object Name	LIKE	Parameter	ObjectNameLike	
<input type="checkbox"/>	AND	Client/Server	Server IP	LIKE	Parameter	ServerIPLike	
<input type="checkbox"/>	AND	Session	Session Start	>=	Parameter	SessionStartsAfter	



## Broad Platform Support

Supported Platforms	Supported Versions
Oracle	8i, 9i, 10g (r1, r2), 11g, 11gR2
Oracle (ASO, SSL)	9i,10g (r1,r2), 11g
Microsoft SQL Server	2000, 2003, 2008
Microsoft SharePoint	2007, 2010
IBM DB2 (Linux, Unix, Linux for System z)	9.1, 9.5, 9.7
IBM DB2 for z/OS	7, 8, 9
IBM DB2 (Windows)	9.1, 9.2, 9.5, 9.7
IBM DB2 for iSeries	V5R2, V5R3, V5R4, V6R1
IBM Informix	7, 9, 10,11, 11.5
Oracle MySQL and MySQL Cluster	4.1, 5.0, 5.1
Sybase ASE	12, 15, 15.5
Sybase IQ	12.6, 15
Teradata	6.x, 12,13
Netezza	4.5
PostgreSQL	8

## InfoSphere Guardium: Chosen by Leading Organizations Worldwide

- 5 of the top 5 global banks
- 2 of the top 3 global retailers
- 3 of the top 5 global insurers
- 2 of the world's favorite beverage brands
- The most recognized name in PCs
- 15 of the world's leading telcos
- Top government agencies
- Top 3 auto maker
- #1 dedicated security company
- Leading energy suppliers
- Major health care providers
- Media & entertainment brands



## Summary & Conclusions

- Traditional log management, network scanners, SIEM and DLP insufficient to secure high-value databases
  - No real-time monitoring at data level to detect unauthorized access
  - Inability to detect fraud at application layer
  - Native logging/auditing require database changes & impact performance
  - No knowledge about DBMS commands, vulnerabilities & structures
- Guardium is the most widely-deployed solution, with ongoing feedback from the most demanding data center environments worldwide
  - Scalable enterprise architecture
  - Broad heterogeneous support
  - 100% visibility and granular control
  - Deep automation to reduce workload
  - Holistic approach

