Mitigate Risk When Dealing with Confidential information and Privacy Compiance

Henry Lee
SWGHK, IBM

IBM Acquires Guardium

- Joining IBM's Information Management business
- Why Guardium? Unique ability to:
  - Safeguard critical enterprise information
  - Reduce operational costs by automating compliance processes
  - Simplify governance with centralized policies for heterogeneous infrastructures
  - Continuously monitor access and changes to high-value databases

Database Monitoring: 3 Key Business Drivers

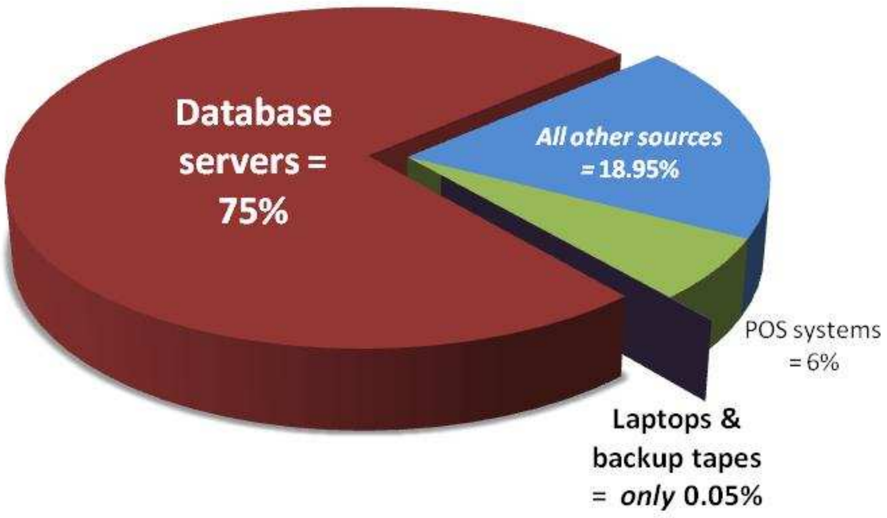
1. **External threats**
   - Prevent theft

2. **Internal threats**
   - Identify unauthorized changes (governance)
   - Prevent data leakage

3. **Compliance**
   - Simplify processes
   - Reduce costs

Database Servers = Vast Majority of Compromised Records

% of Records Breached (2009)



2009 Data Breach Report from Verizon Business RISK Team

http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

Online data = 99.9% of all compromised records

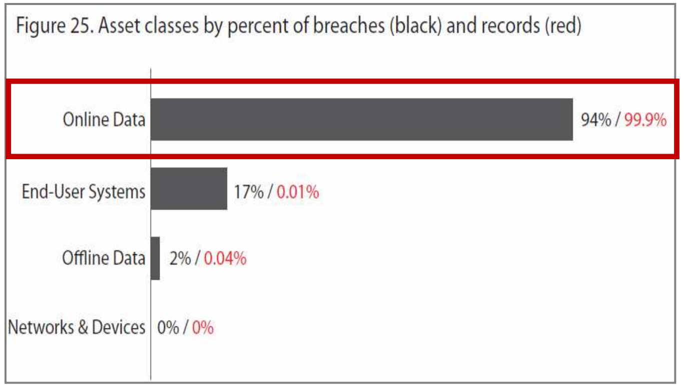
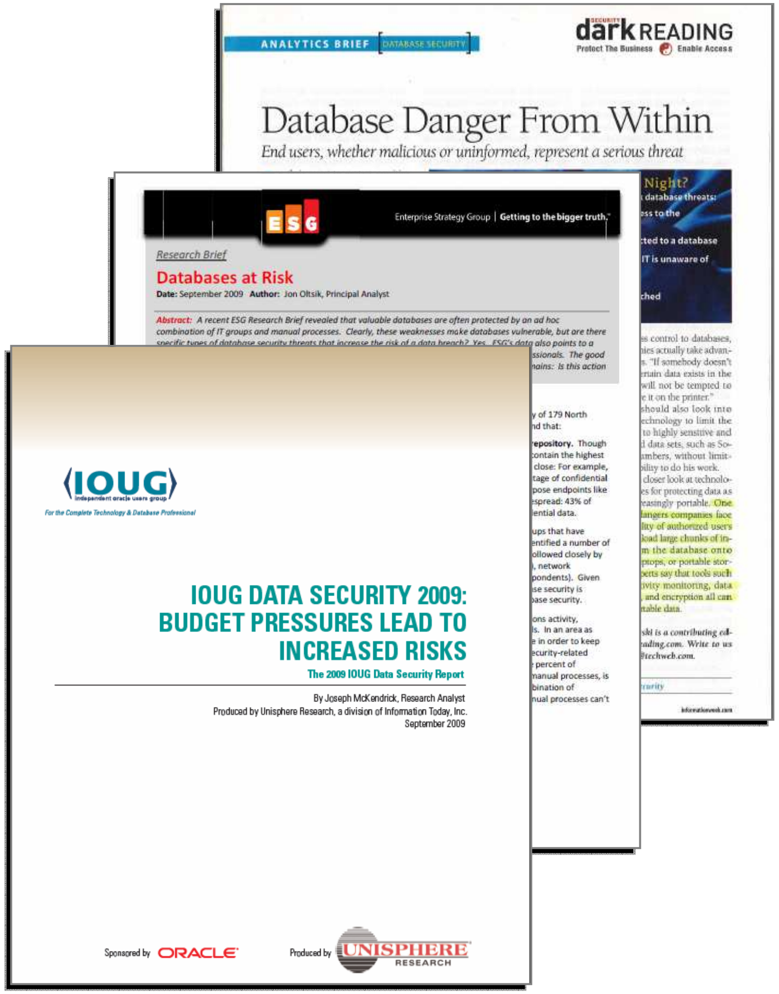


Figure 25. Asset classes by percent of breaches (black) and records (red)

"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."**

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]

SECURITY darkREADING
Protect The Business Enable Access

Database Danger From Within

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

Night?
database threats:
ess to the
cted to a database
IT is unaware of
ched

es control to databases,
nies actually take advan-
s. "If somebody doesn't
ertain data exists in the
will not be tempted to
e it on the printer."
should also look into
echnology to limit the
to highly sensitive and
d data sets, such as So-
umbers, without limit-
bility to do his work.
closer look at technolo-
es for protecting data as
easingly portable. One
dangers companies face
lity of authorized users
load large chunks of in-
m the database onto
ptops, or portable stor-
perts say that tools such
tivity monitoring, data
, and encryption all can
rtable data.

ski is a contributing ed-
ading.com. Write to us
@techweb.com.

curity

informationweek.com

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
ssionals. The good
nains: Is this action

y of 179 North
nd that:

repository. Though
contain the highest
close: For example,
tage of confidential
pose endpoints like
espread: 43% of
ential data.

ups that have
entified a number of
ollowed closely by
, network
pondents). Given
se security is
base security.

ons activity,
ls. In an area as
e in order to keep
ecurity-related
percent of
manual processes, is
bination of
nual processes can't

⟨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.guardium.com/index.php/landing/866/

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

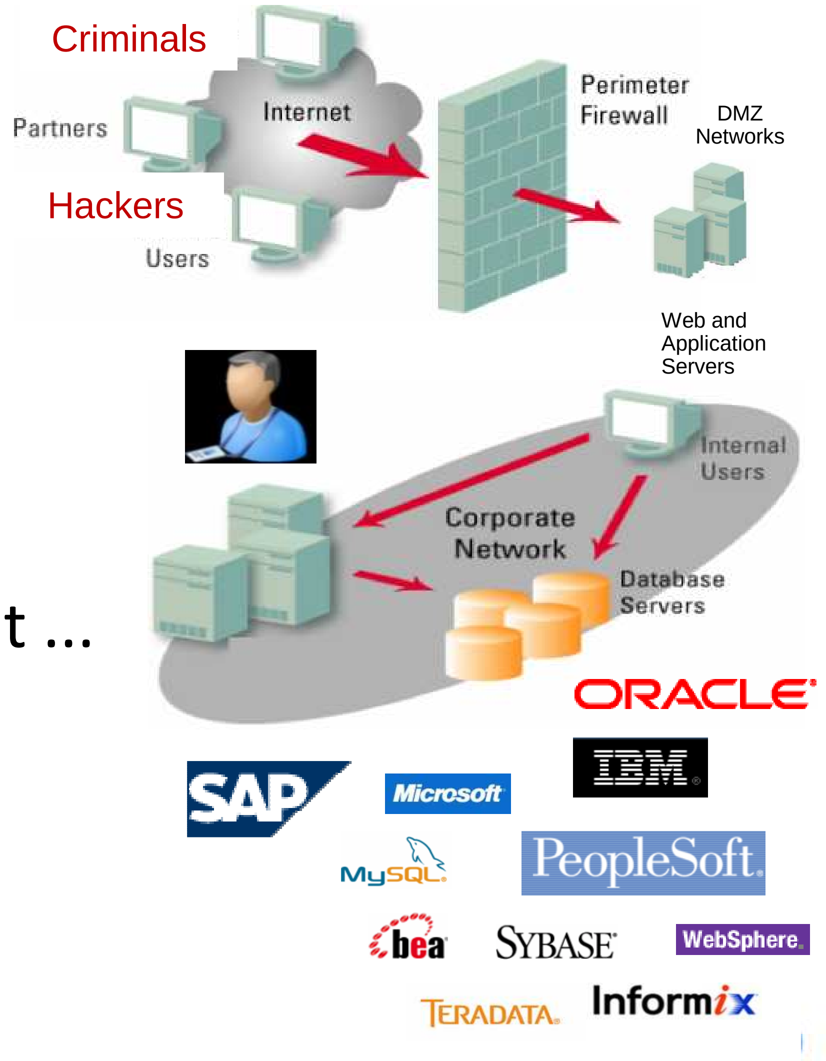
The Compliance Mandate

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

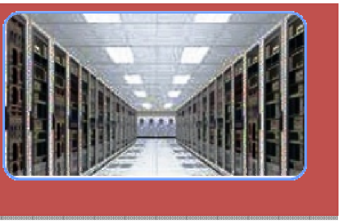
The Complexity & Visibility Challenges

- Heterogeneous & distributed
- Multiple access paths
- Firewalls, IDS/IPS can't prevent traffic that appears to be legitimate
- Most organizations have formal data security policies but ...
  - No practical enforcement mechanisms
  - No visibility into what's really going on -- especially with privileged users



Top Data Protection Challenges

Where is my sensitive data - and who's accessing it (including privileged users)?

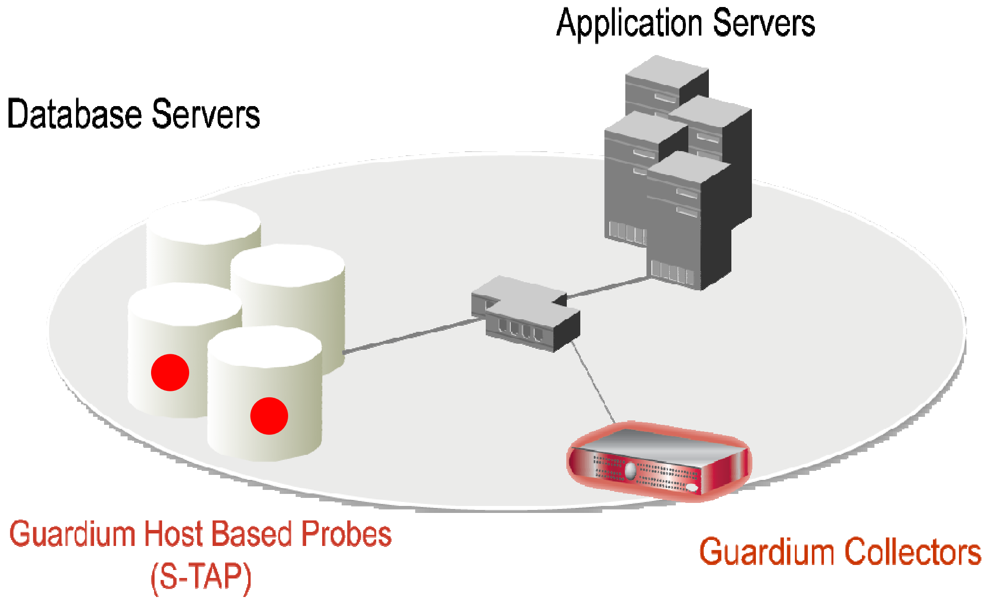


How can I enforce access control & change control policies for databases?

How do I check for vulnerabilities and lock-down database configurations?

How do I reduce costs by automating & centralizing compliance controls?

Real-Time Database Monitoring



Application Servers

Database Servers

Guardium Host Based Probes (S-TAP)

Guardium Collectors

ORACLE

IBM DB2

SQL Server

TERADATA

SYBASE

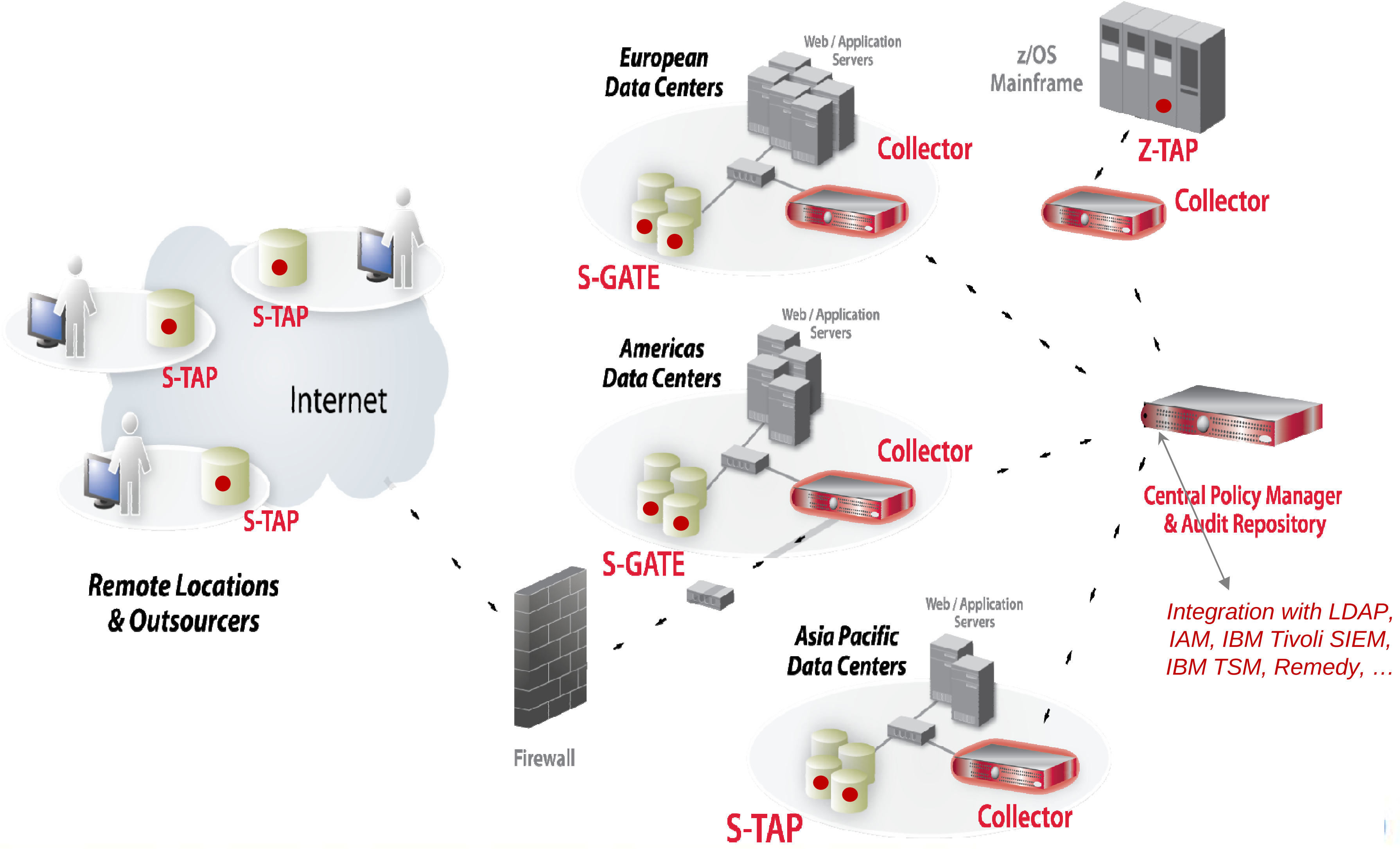
MySQL

Informix

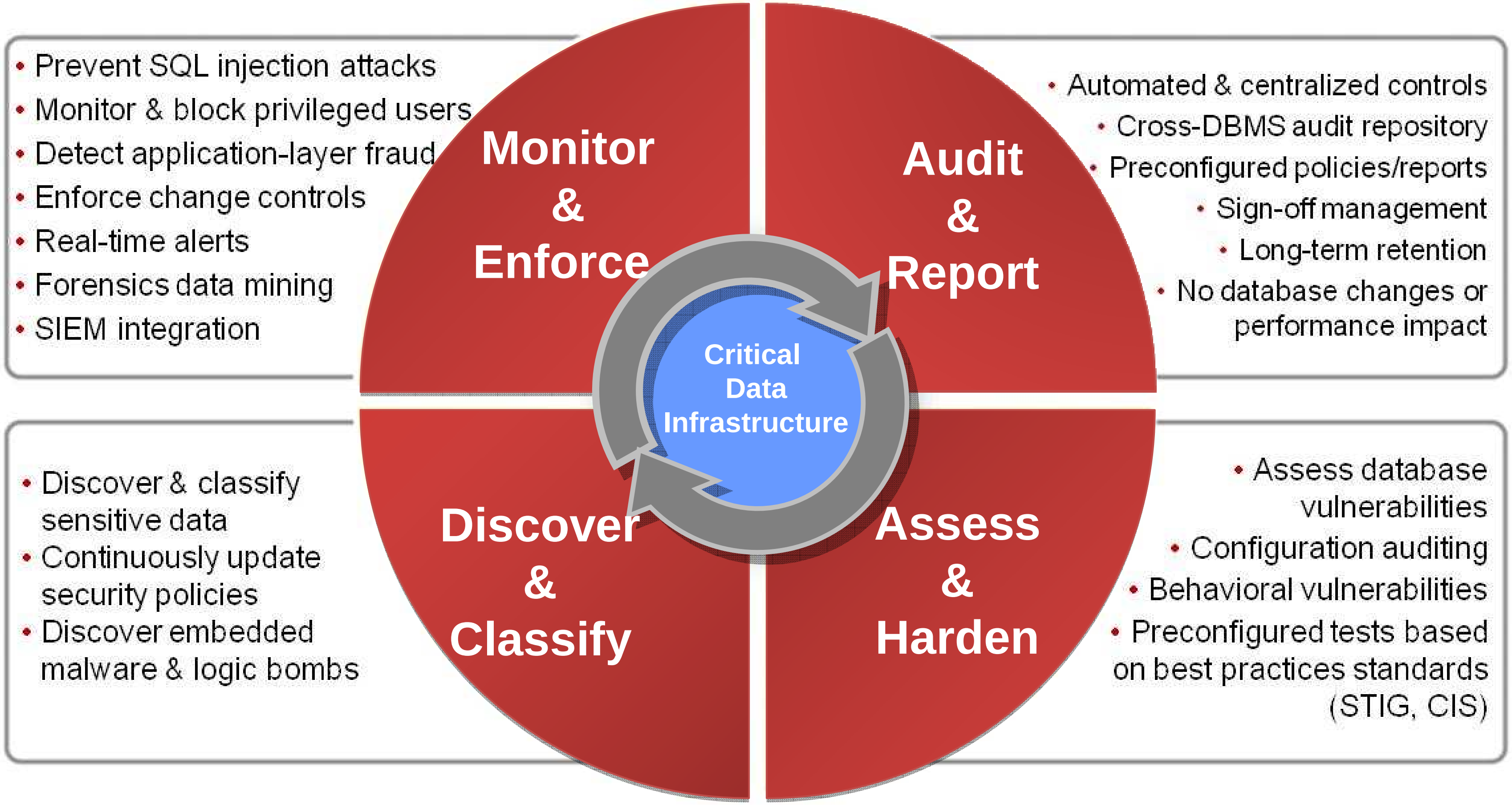
- Non-invasive architecture
  - Outside database
  - Minimal performance impact (2-3%)
  - No DBMS or application changes
- Cross-DBMS solution
- 100% visibility including local DBA access

- 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 Full Lifecycle



- Prevent SQL injection attacks
- Monitor & block privileged users
- Detect application-layer fraud
- Enforce change controls
- Real-time alerts
- Forensics data mining
- SIEM integration

- Automated & centralized controls
- Cross-DBMS audit repository
- Preconfigured policies/reports
- Sign-off management
- Long-term retention
- No database changes or performance impact

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

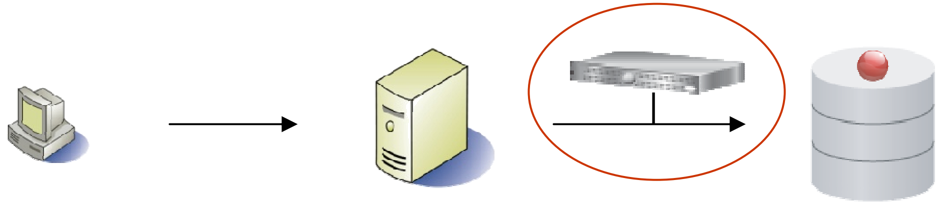
- Assess database vulnerabilities
- Configuration auditing
- Behavioral vulnerabilities
- Preconfigured tests based on best practices standards (STIG, CIS)

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?

Continuous Fine-grained Auditing and Security

All SQL traffic contextually analyzed & filtered in real-time to provide specific information required by auditors

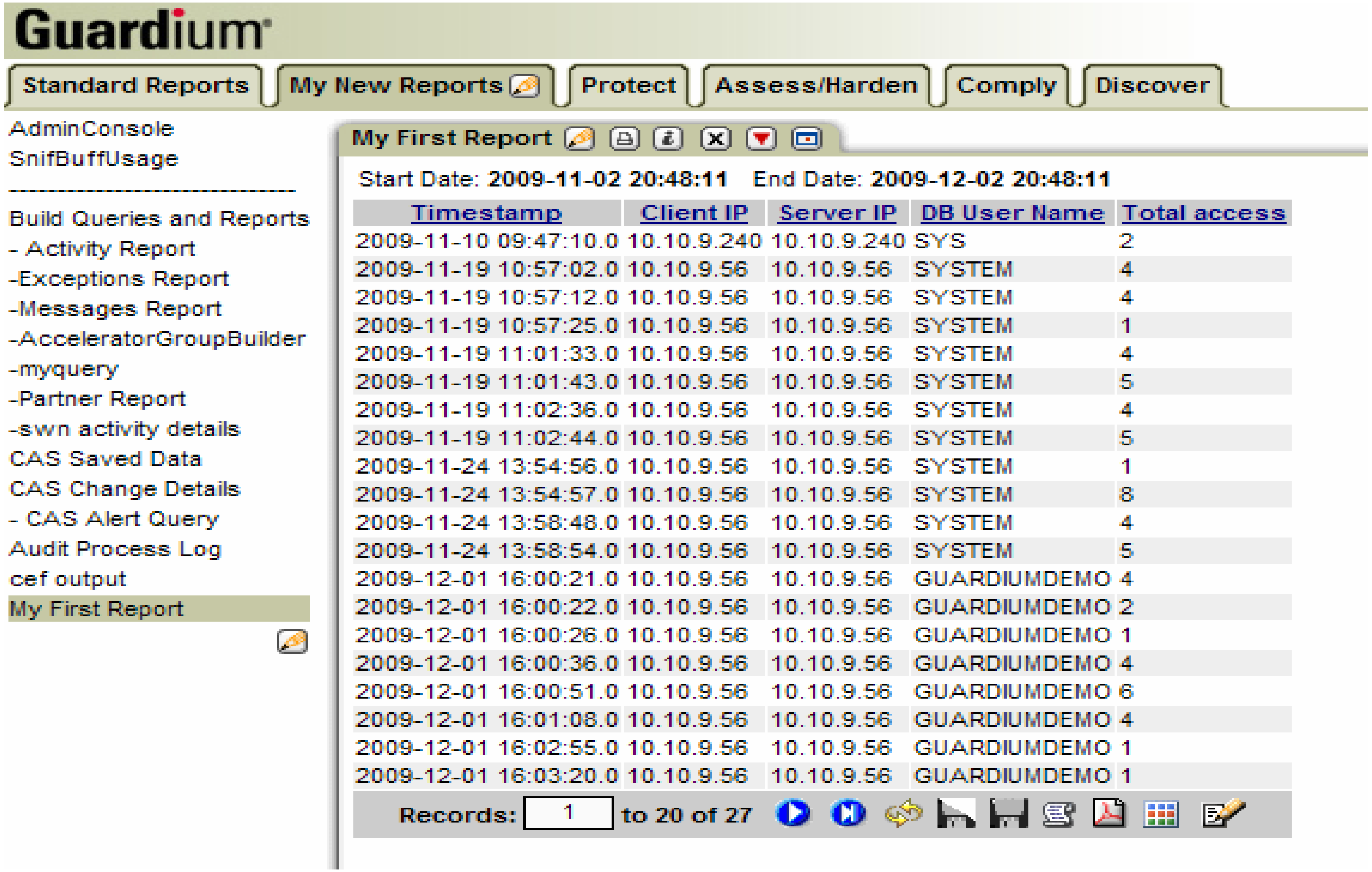


Client IP
Client host name
Domain login
Client OS
MAC
TTL
Origin
Failed logins

Server IP
Server port
Server name
Session
SQL patterns
Network protocol
Server OS
Timestamp
Access programs
App User ID

ALL SQL commands
Fields
Objects
Verbs
DDL
DML
DCL
DB user name
DB version
DB type
DB protocol
Origin
DB errors
SELECTs

Real time report



My First Report

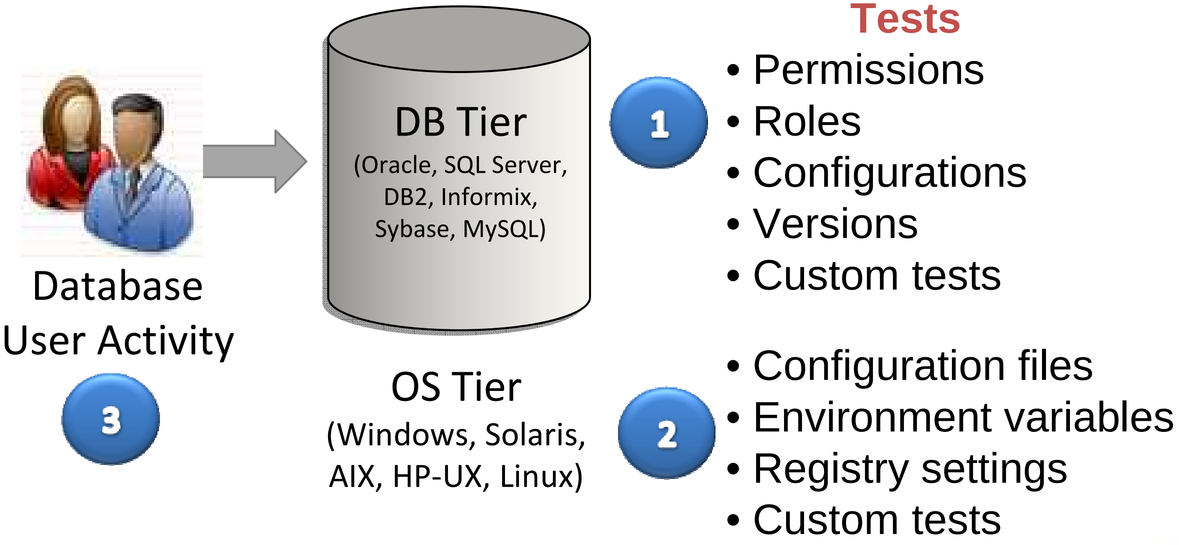
Start Date: **2009-11-02 20:48:11** End Date: **2009-12-02 20:48:11**

Timestamp	Client IP	Server IP	DB User Name	Total access
2009-11-10 09:47:10.0	10.10.9.240	10.10.9.240	SYS	2
2009-11-19 10:57:02.0	10.10.9.56	10.10.9.56	SYSTEM	4
2009-11-19 10:57:12.0	10.10.9.56	10.10.9.56	SYSTEM	4
2009-11-19 10:57:25.0	10.10.9.56	10.10.9.56	SYSTEM	1
2009-11-19 11:01:33.0	10.10.9.56	10.10.9.56	SYSTEM	4
2009-11-19 11:01:43.0	10.10.9.56	10.10.9.56	SYSTEM	5
2009-11-19 11:02:36.0	10.10.9.56	10.10.9.56	SYSTEM	4
2009-11-19 11:02:44.0	10.10.9.56	10.10.9.56	SYSTEM	5
2009-11-24 13:54:56.0	10.10.9.56	10.10.9.56	SYSTEM	1
2009-11-24 13:54:57.0	10.10.9.56	10.10.9.56	SYSTEM	8
2009-11-24 13:58:48.0	10.10.9.56	10.10.9.56	SYSTEM	4
2009-11-24 13:58:54.0	10.10.9.56	10.10.9.56	SYSTEM	5
2009-12-01 16:00:21.0	10.10.9.56	10.10.9.56	GUARDIUMDEMO	4
2009-12-01 16:00:22.0	10.10.9.56	10.10.9.56	GUARDIUMDEMO	2
2009-12-01 16:00:26.0	10.10.9.56	10.10.9.56	GUARDIUMDEMO	1
2009-12-01 16:00:36.0	10.10.9.56	10.10.9.56	GUARDIUMDEMO	4
2009-12-01 16:00:51.0	10.10.9.56	10.10.9.56	GUARDIUMDEMO	6
2009-12-01 16:01:08.0	10.10.9.56	10.10.9.56	GUARDIUMDEMO	4
2009-12-01 16:02:55.0	10.10.9.56	10.10.9.56	GUARDIUMDEMO	1
2009-12-01 16:03:20.0	10.10.9.56	10.10.9.56	GUARDIUMDEMO	1

Records: 1 to 20 of 27

Vulnerability & Configuration Assessment

- 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

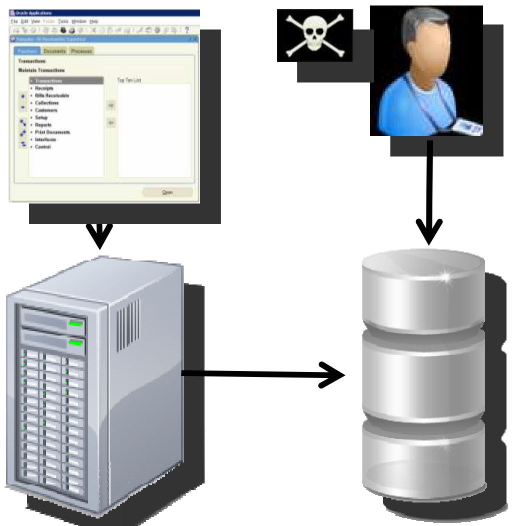
1

- Permissions
- Roles
- Configurations
- Versions
- Custom tests

2

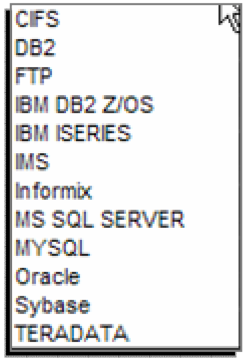
- Configuration files
- Environment variables
- Registry settings
- Custom tests

Fine-Grained Policies with Real-Time Alerts

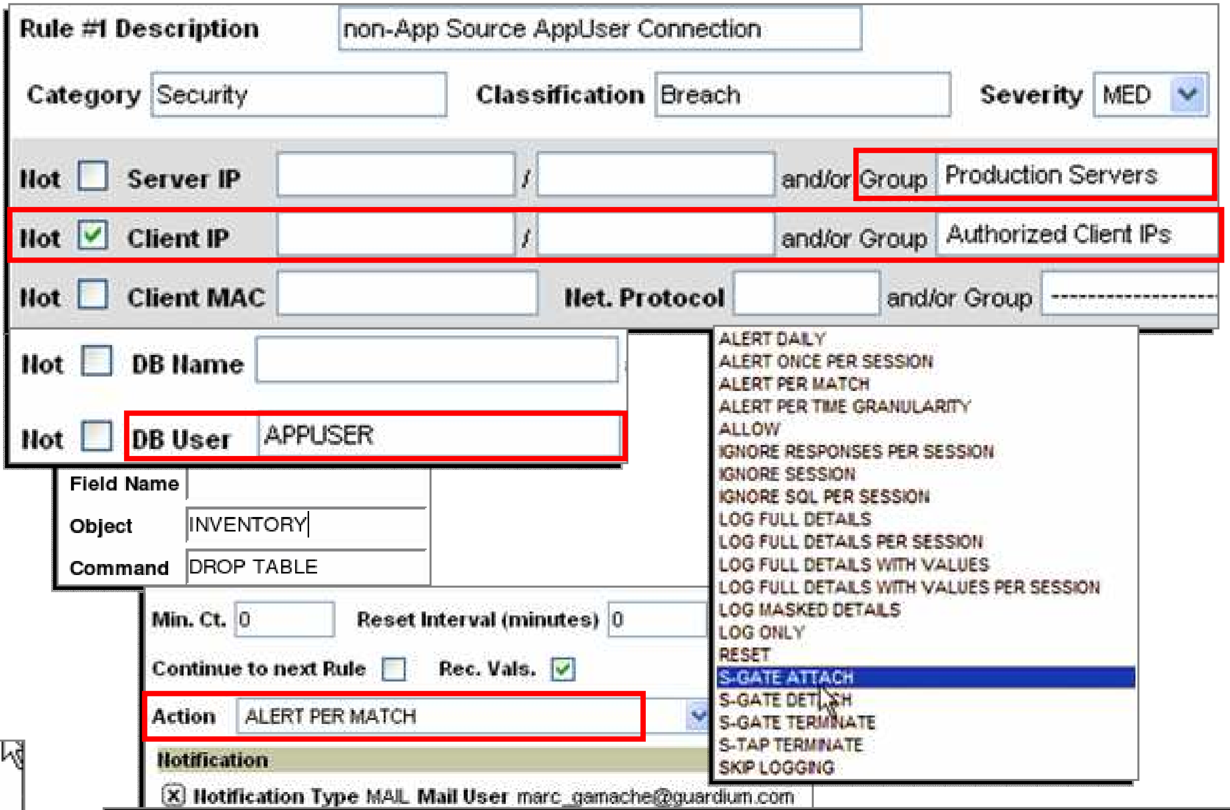


Application Server 10.10.9.244

Database Server 10.10.9.56



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

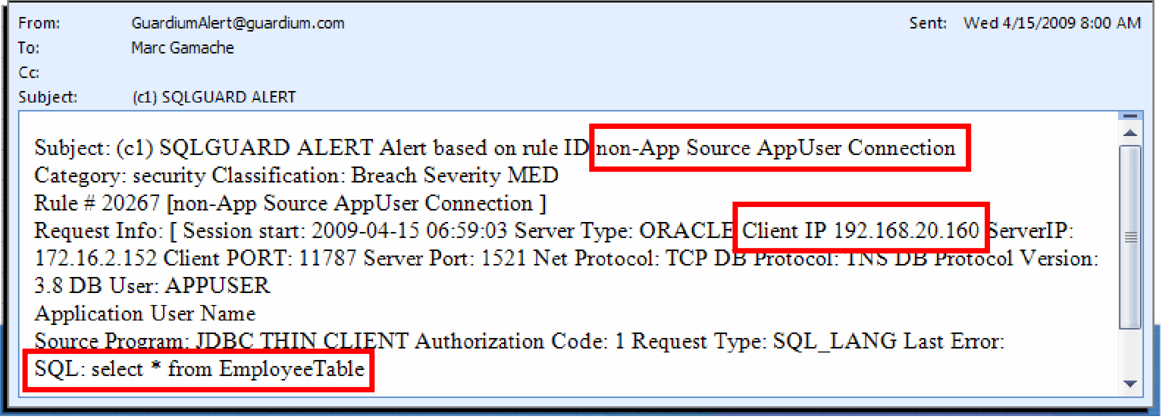
Min. Ct. 0 Reset Interval (minutes) 0

Continue to next Rule □ Rec. Vals. ☑

Action: ALERT PER MATCH

Notification

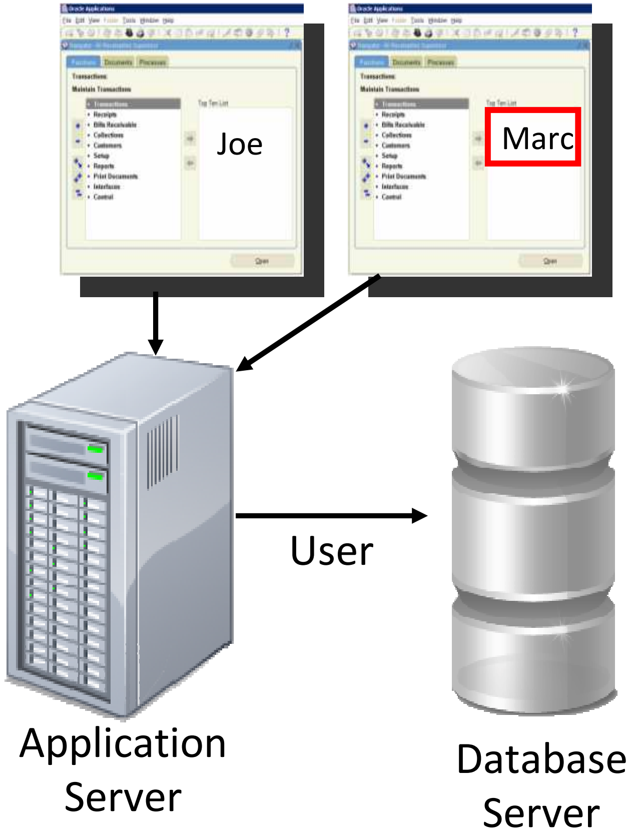
☒ Notification Type MAIL Mail User marc_gamache@guardium.com

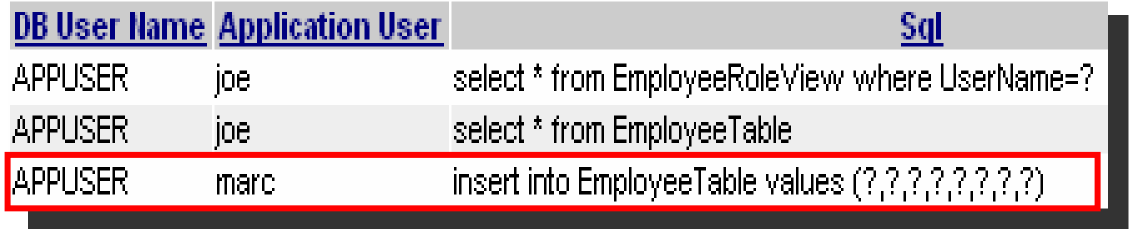


From: GuardiumAlert@guardium.com
Sent: Wed 4/15/2009 8:00 AM
To: Marc Gamache
Cc:
Subject: (c1) SQLGUARD ALERT

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

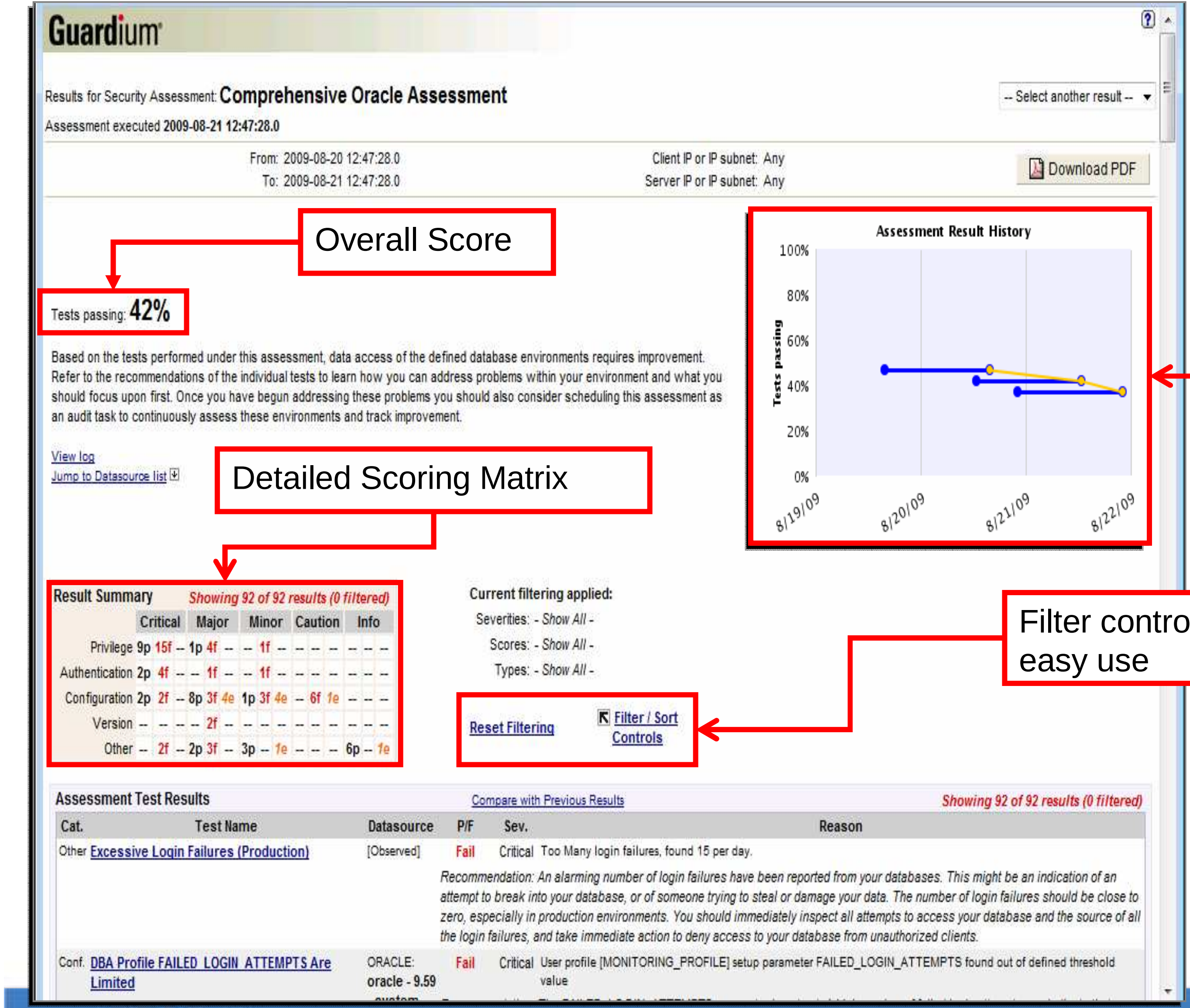




DB User Name	Application User	Sql
APPUSER	joe	select * from EmployeeRoleView where UserName=?
APPUSER	joe	select * from EmployeeTable
APPUSER	marc	insert into EmployeeTable values (?,?,?,?,?,?,?,?,?)

- ***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….)

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

Tests passing: **42%**

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.

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 -*

Assessment Test Results

Showing 92 of 92 results (0 filtered)

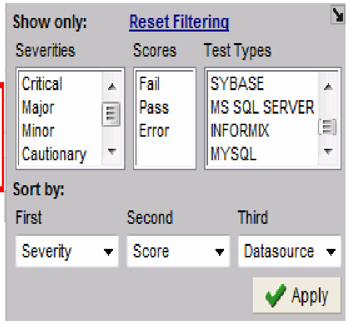
Cat.	Test Name	Datasource	P/F	Sev.	Reason
Other	Excessive Login Failures (Production)	[Observed]	Fail	Critical	Too Many login failures, found 15 per day. *Recommendation: An alarming number of login failures have been reported from your databases. This might be an indication of an attempt to break into 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

Overall Score

Detailed Scoring Matrix

Historical Progress or Regression

Filter control for easy use



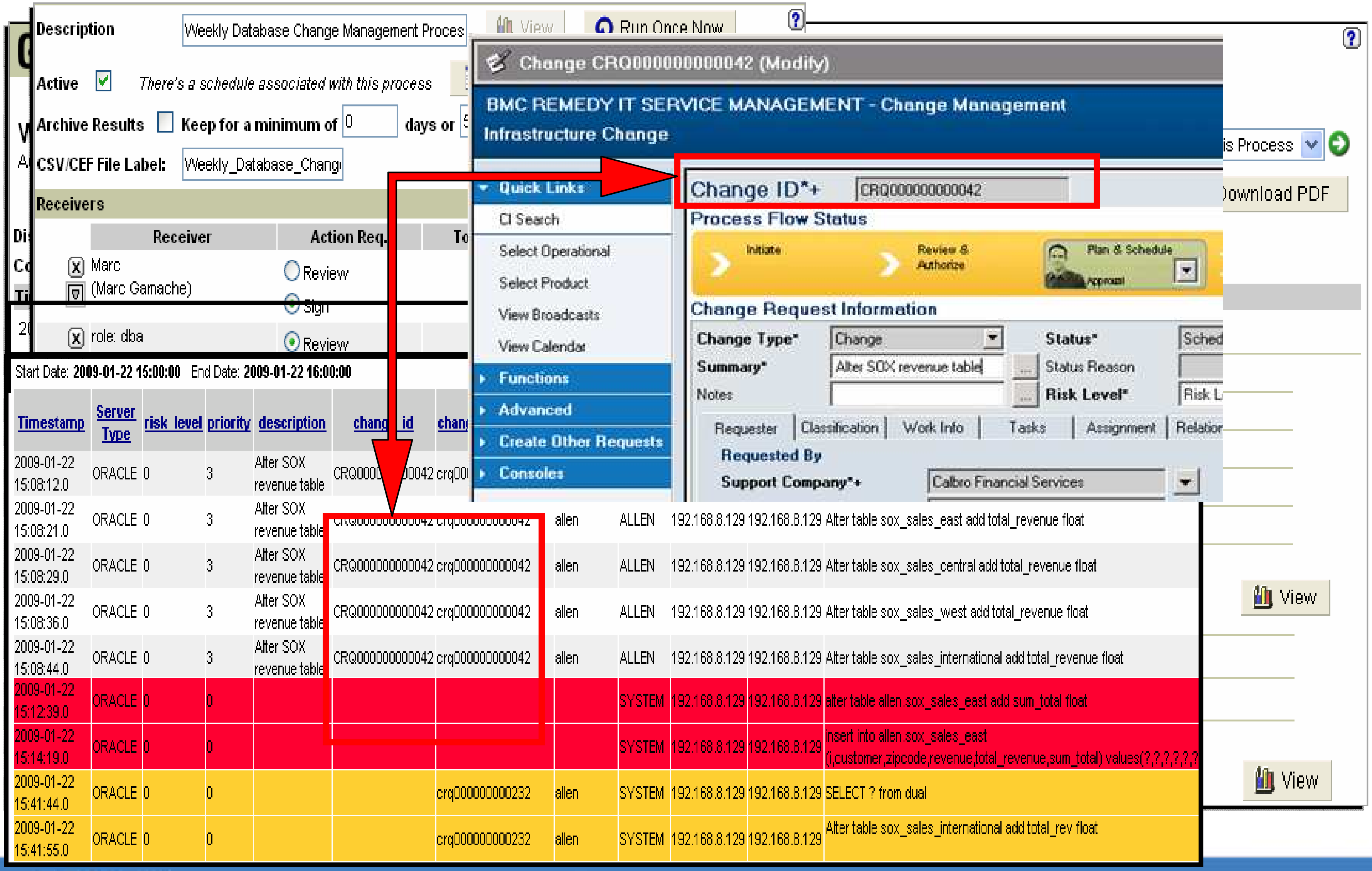
Show only:

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

Sort by:

First	Second	Third
Severity	Score	Datasource

Automated Sign-offs & Escalations for Compliance



Description: Weekly Database Change Management Proces

View | Run Once Now

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

Archive Results □ Keep for a minimum of 0 days or

CSV/CEF File Label: Weekly_Database_Chang

Receivers

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

Change CRQ000000000042 (Modify)

BMC REMEDY IT SERVICE MANAGEMENT - Change Management

Infrastructure Change

Quick Links: CI Search, Select Operational, Select Product, View Broadcasts, View Calendar; Functions; Advanced; Create Other Requests; Consoles

Change ID*+ CRQ000000000042

Process Flow Status: Initiate › Review & Authorize › Plan & Schedule (Approval)

Change Request Information

Change Type*: Change

Status*: Sched

Summary*: Alter SOX revenue table

Status Reason:

Notes:

Risk Level*: Risk L

Requester | Classification | Work Info | Tasks | Assignment | Relation

Requested By

Support Company*+: Calbro Financial Services

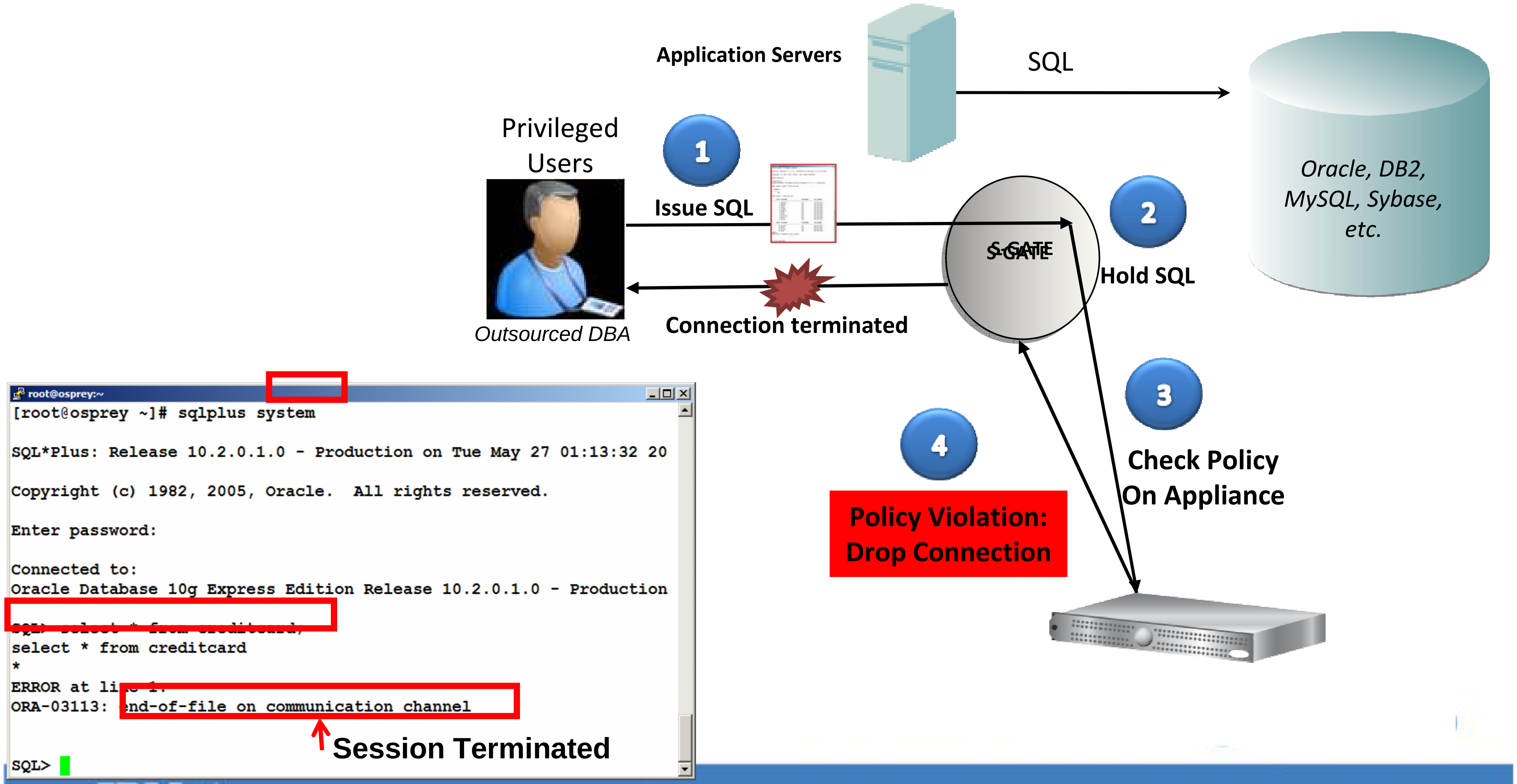
is Process | Download PDF | View | View

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

Timestamp	Server Type	risk_level	priority	description	chang_id	chan					
2009-01-22 15:08:12.0	ORACLE	0	3	Alter SOX revenue table	CRQ0000 00042	crq00					
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

S-GATE: Blocking Access 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



```
[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> 
```

Databases can be monitored

Supported Platforms	Supported Versions
Oracle	8i, 9i, 10g (r1, r2), 11g, 11i
Microsoft SQL Server	2000, 2005, 2008
IBM DB2 UBD (Windows, Unix, z/Linux)	8.0, 8.2, 9.1, 9.5
IBM DB2 for z/OS	7, 8, 9, 9.5
IBM DB2 UBD for iSeries (AS/400)	V5R2, V5R3, V5R4, V6R1
IBM Informix	7, 8, 9, 10,11
MySQL	4.1, 5.0, 5.1
Sybase ASE	12, 15
Sybase IQ	12.6
Teradata	6.01, 6.02

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 & 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/auditing require database changes & impact performance
- 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 & granular control
  - Deep automation to reduce workload
  - Holistic approach

Thank You!