



# Enterprise Database Security & Monitoring

*Data Management*

Gerald Tan  
IBM Singapore

**Guardium**<sup>®</sup>  
SAFEGUARDING DATABASES™ | AN IBM COMPANY

# Database Monitoring: 3 Key Business Drivers

## 1. Internal threats

- Identify unauthorized changes (governance)
- Prevent data leakage



## 2. External threats

- Prevent theft



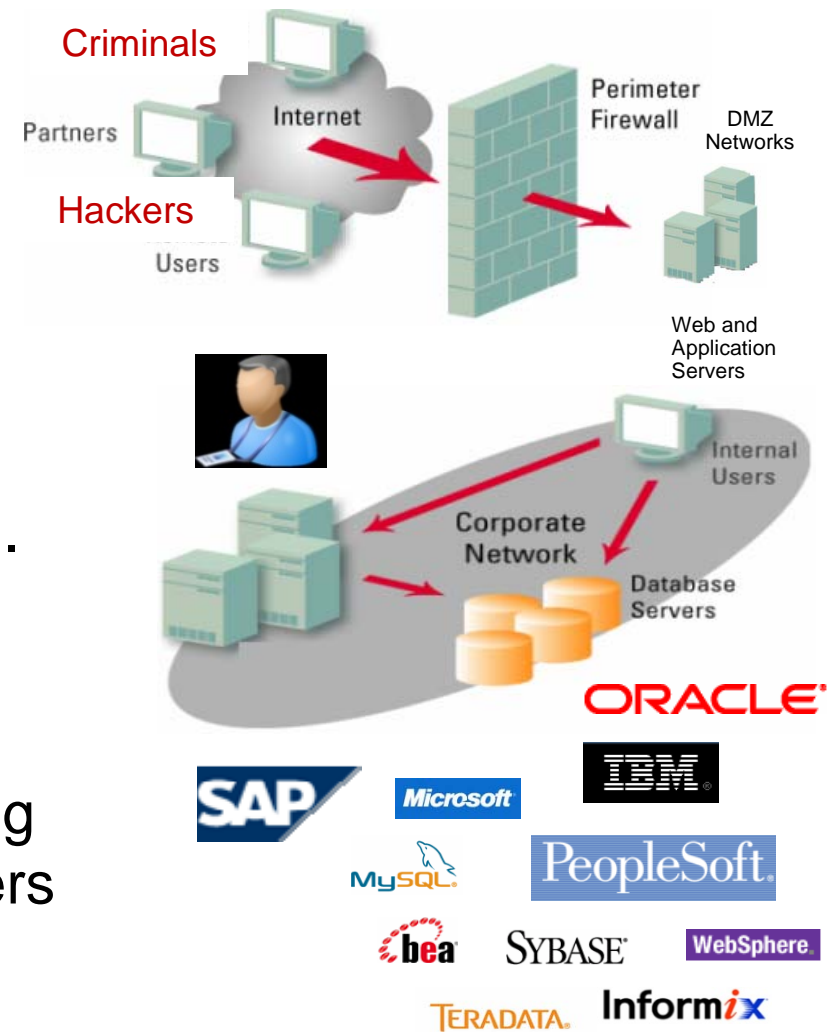
## 3. Compliance

- Simplify processes
- Reduce costs



## The Complexity & Visibility Challenge

- Heterogeneous & distributed
- Multiple access paths
- Firewalls 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?

# 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



## COMPLIANCE AUDIT

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



## SECURITY OPERATIONS

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



## APPLICATION & DATABASE

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

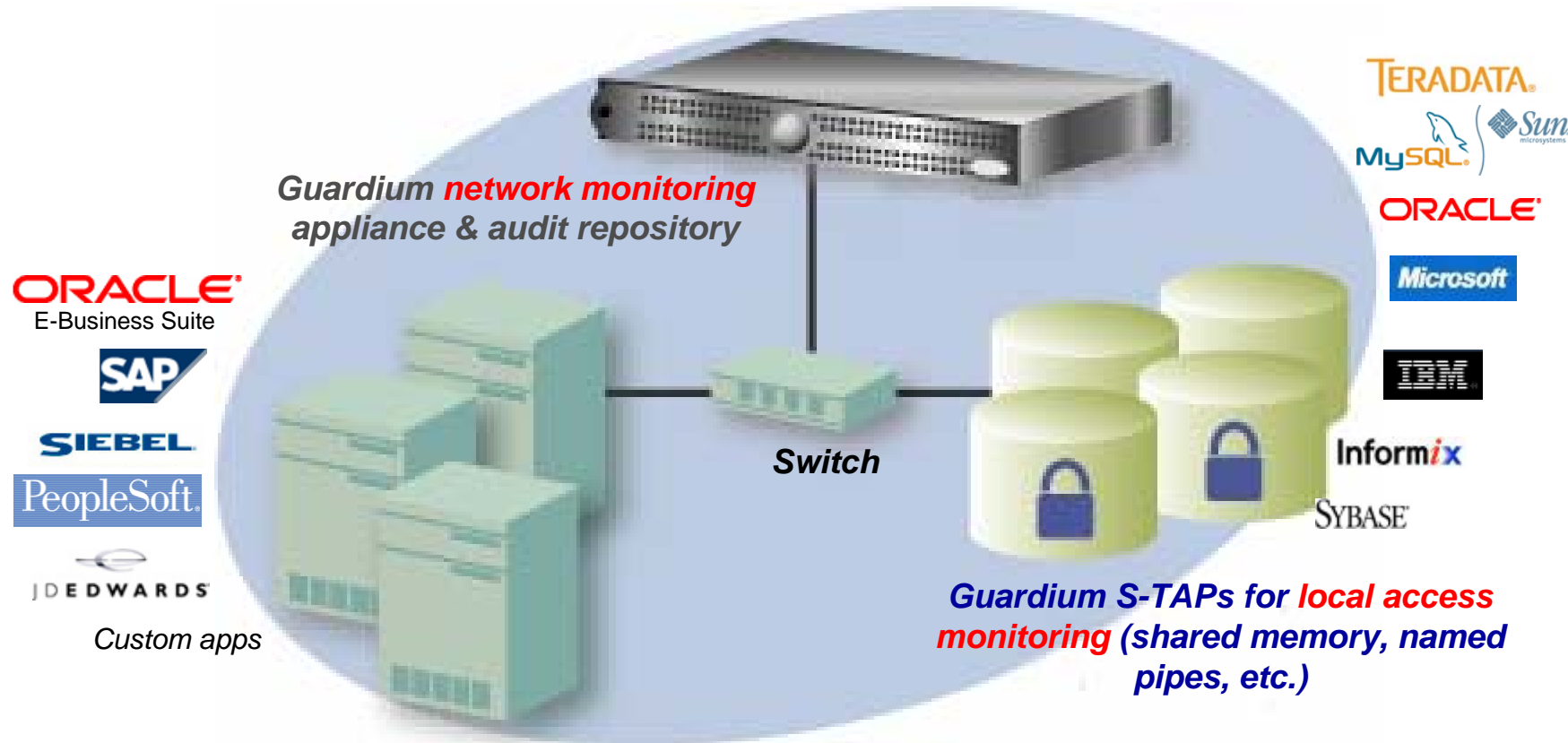
Guardium: 100% Visibility &  
Unified View

**Guardium**<sup>®</sup>

SAFEGUARDING DATABASES™ | AN IBM® COMPANY

© 2009 IBM Corporation

# Guardium Solution

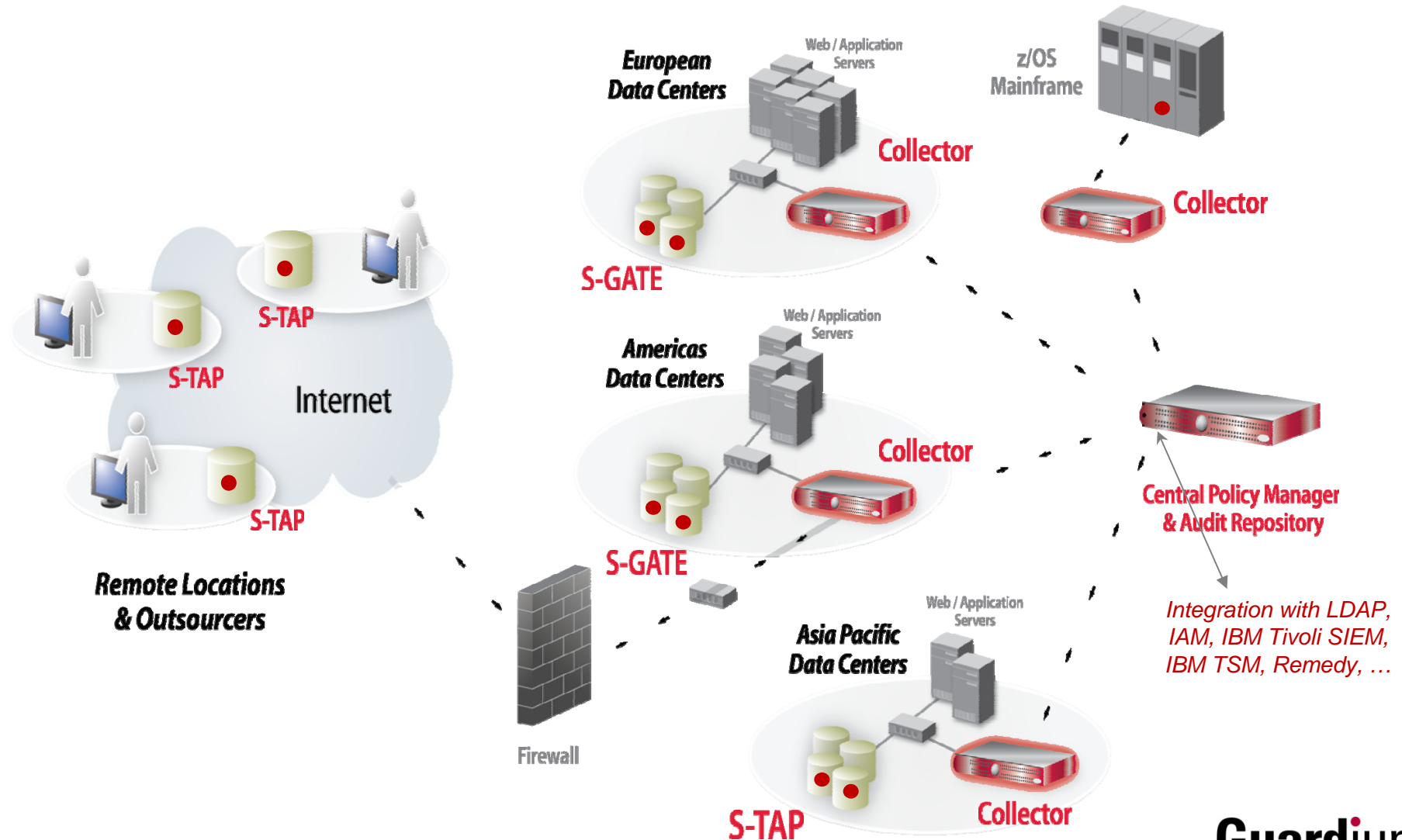


- Non-invasive
- No DBMS changes
- Minimal impact
- Does not rely on traditional DBMS-resident logs that can easily be disabled by DBAs

- Granular policies & monitoring
  - *Who, what, when, how*
- Real-time alerting
- Monitors all activities including local access by privileged users

**Guardium**<sup>®</sup>  
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

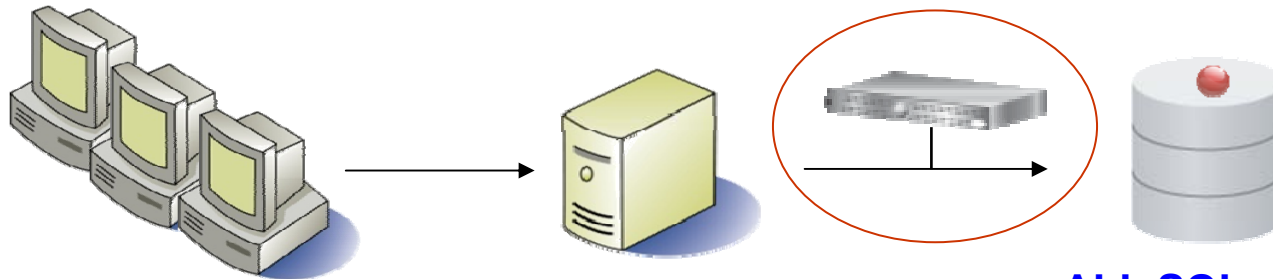
# Scalable Enterprise-wide Multi-Tier Architecture





# 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

## Provide insight such as . . .

- **Who** is changing database schemas or dropping tables?
- **When** there are 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?
- **What** are the access patterns based on time of day?
- **What** database errors are being generated?
- **What** is the exposure to sensitive objects?

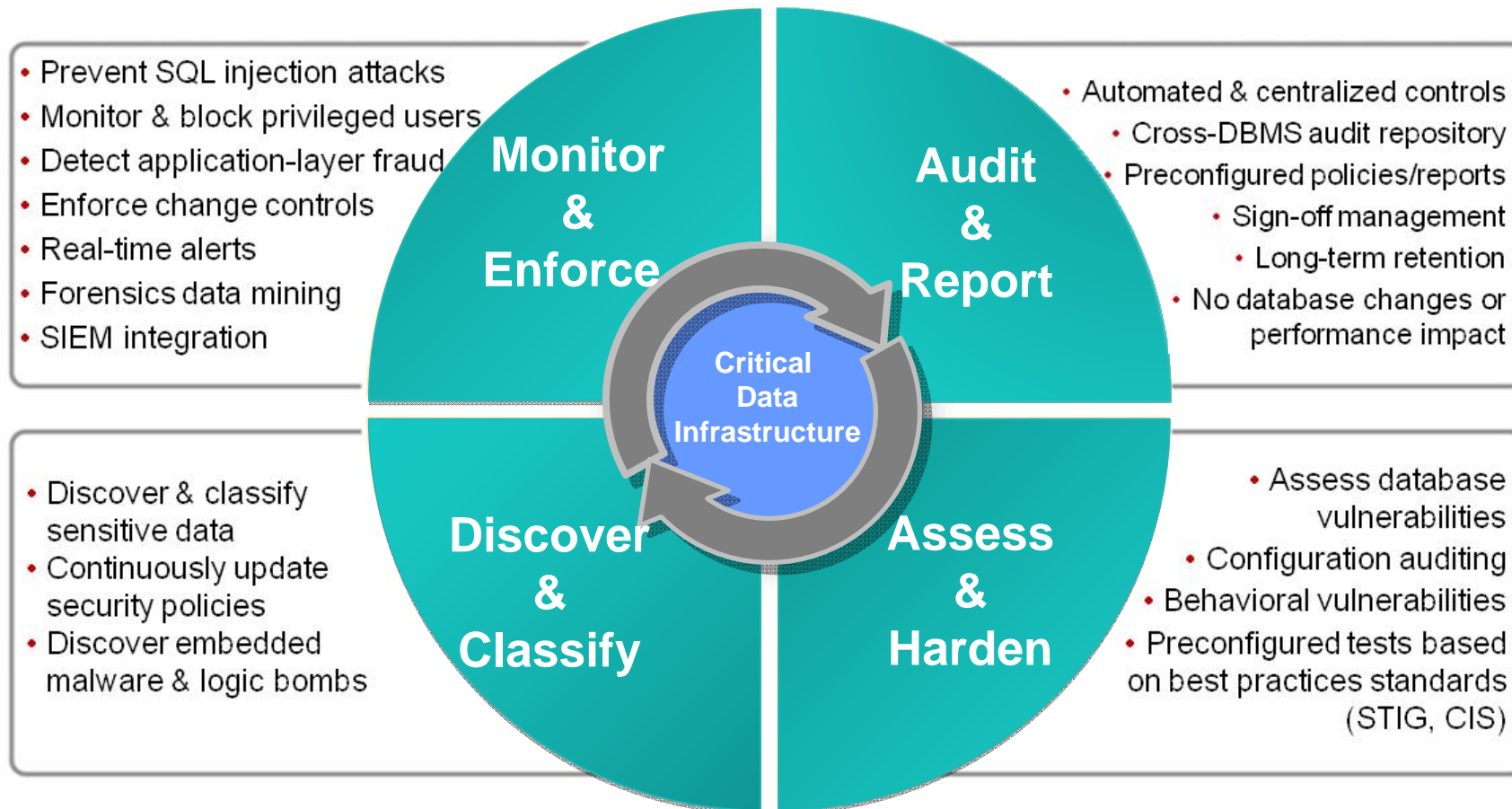


**Guardium**<sup>®</sup>

SAFEGUARDING DATABASES™ | AN IBM® COMPANY

© 2009 IBM Corporation

# Addressing the Full Lifecycle



# Policies

**Policy Rules**

**Production Database Policy** Filter: [ ] [ ] [ ] [ ] [ ] [ ] [ ]

Expand All Collapse All Select All Unselect All Remove Selected Copy Rules ...

- 1 Baseline : baseline 8 hours (Action: Accept and don't cont. to next Rule)
- 2 Access Rule: Log full Details
- 3 Access Rule: Unauthorized user access to sensitive data
- 4 Exception Rule: Alert on Failed Login
- 5 Exception Rule: Alert on SQL Errors
- 6 Extrusion Rule: Unauthorized Data Privacy Access
- 7 Extrusion Rule: Unauthorized CreditCard Access

+ Add Access Rule... + Add Exception Rule... + Add Extrusion Rule...

Rule Suggestion Suggest from DB ACL Rule minimum ct. 0 Object Group minimum ct. 1 Suggest Rules

Cancel Policy Simulator Done

# 1. Access Policy – Very Granular to Meet Customer Requirements

Rule #4 Description: Terminate Connection

Category: Policy Classification: Violation Severity: HIGH

Not  Server IP / and/or Group: Production Servers

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

Not  Client MAC / and/or Group: -----

DB Type: Oracle

Not  Service Name / and/or Group: -----

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

Not  DB User / and/or Group: (Public) Admin Users

Not  App. User / and/or Group: Oracle EBS AppUser Group

Not  OS User / and/or Group: Unauthorized OS Users

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

Not  Field Name / and/or Group: Sensitive Columns

Not  Object / and/or Group: Financial Objects

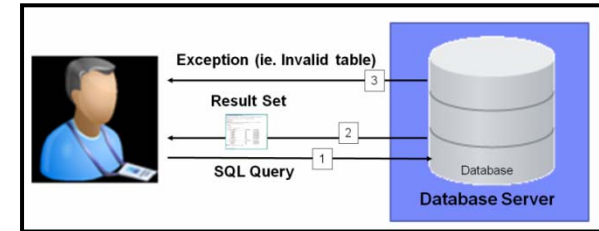
Not  Command / and/or Group: (Public) DML Commands

Min. Ct. 0 Reset Interval (minutes) 0

Continue to next Rule  Rec. Vals.

Action: S-GATE TERMINATE

- 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



Which Servers

Which Databases

Which Users

Which Fields

Which Tables

Which SQL Commands

- What Action?
- Allow, Log, Log Full Details, Log full Details with Values
- Alert, Ignore, Terminate **Guardium**

# Dashboard

Guardium
10:12 Edit Account: admin Customize Logout

System View
Administration Console
Tools
Daily Monitor
Guardium Monitor
Tap Monitor
Incident Management

### STAP Status Monitor

S-Tap Host	S-Tap Version	DB Server Type	Status	Last Response Received	Primary Host Name	KTAP	TEE	MSS Shm	DB2 Shm	Local TCP	Pipes	Encrypted?
10.11.40.13	7.0.1.38	MSSQL	Active	2010-07-02 10:12:25.0	10.11.40.254	No	No	Yes	No	Yes	Yes	Unencrypted
10.11.40.138	STAP-7.0.0-20091203-1344	ORACLE	Active	2010-07-02 10:12:27.0	10.11.40.254	Yes	No	No	No	No	No	Unencrypted
10.11.40.148	7.0.1.38	ORACLE	Active	2010-07-02 10:12:25.0	10.11.40.254	No	No	No	No	Yes	Yes	Unencrypted
10.11.40.243	7.0.1.38	MYSQL	Active	2010-07-02 10:12:25.0	10.11.40.254	No	No	No	No	Yes	No	Unencrypted
10.11.40.83	7.0.1.38	DB2	Active	2010-07-02 10:12:25.0	10.11.40.254	No	No	No	Yes	Yes	No	Unencrypted

Records: 1 to 5 of 5

Aliases: OFF

### Request Rate

From 2010-07-02 08:12:30 To 2010-07-02 10:12:30

Aliases: OFF

### CPU Usage

From 2010-07-02 08:12:31 To 2010-07-02 10:12:31

Aliases: OFF

### Logins to Guardium

Start Date: 2010-07-01 10:12:32 End Date: 2010-07-02 10:12:32

User Name	Login Succeeded	Login Date And Time	Logout Date And Time	Host Name	Remote Address
admin	0	2010-07-01 15:07:14.0	2010-07-01 15:07:14.0	guardiumvm	10.11.40.83
admin	0	2010-07-01 15:07:28.0	2010-07-01 15:07:28.0	guardiumvm	10.11.40.83
admin	0	2010-07-02 10:00:37.0	2010-07-02 10:00:37.0	guardiumvm	10.11.33.236
admin	1	2010-07-01 15:07:34.0		guardiumvm	10.11.40.83
admin	1	2010-07-01 16:41:33.0	2010-07-01 17:45:33.0	guardiumvm	10.11.40.83

Records: 1 to 5 of 11

### Current Status Monitor

```
procs -----memory-----swap-----io-----system-----cpu-----
r  b  swpd  free  buff  cache  si  so  bi  bo  in  cs  us  sy  id  wa  st
0  0      0 314732 166148 879652  0  0  0  4  639 1317  0  2  97  1  0
```

SQL Server Teradata

0 0

219185 0

Oracle MySQL

0 0

5585 15712

DB2 XML

0 0

0 0

Sybase IMS

0 0

0 0

Informix Files/Other

0 0

0 0

Analysis Engine

0-0

462011

Free Disk Space

100GB

DB 0% Full

Unit is configured as: [Inspecting Network][Inspecting Using STAPs][Standalone][Not Inline]

# DB Activities

Guardium (guardiumvm) - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Favorites Print

Address <https://10.11.40.254:8443/sqlguard/media-type/html/user/audit/page/default.psml> Go

**Guardium** 10:20 [Edit Account: audit](#) [Customize](#) [Logout](#) G2000 - Standalone Unit

**View** **Monitor/Audit** **Discover** **Assess/Harden** **Comply** **Protect**

**Build Audit Policies** **Build Reports** **My New Reports** **Privacy Sets** **POC**

01 - DB activities

02 - correlate DB activity

03 - Separation of duties

04 - DBA activity

06 - Restrict DB user to certain IP

08 - Login Failed

09 - ILS\_USER\_NAMAD

10 - local access

11 - record affected

01 - DB activities

Start Date: 2010-07-01 10:15:09 End Date: 2010-07-02 10:15:09

Server IP	Server Type	Service Name	Database Name	DB User Name	Count of Sql	Total access
10.11.40.13	MS SQL SERVER			SYSTEM	13	77870
10.11.40.13	MS SQL SERVER		SDMSUAT	SA	79	62441
10.11.40.13	MS SQL SERVER		SDMSUAT	SYSTEM	30	10622
10.11.40.138	ORACLE	ILSPROD		DUMMY_USER	6	84
10.11.40.138	ORACLE	ILSPROD		ECOMSINT	2	16
10.11.40.138	ORACLE	ILSPROD		ILS_MANAGER	184	66791
10.11.40.138	ORACLE	ILSPROD		POC_USER	12	15
10.11.40.138	ORACLE	ORACLEILSPROD		POC_USER	16	97
10.11.40.138	ORACLE	ORACLEILSTEST		POC_USER	1	1
10.11.40.148	ORACLE	RUSHUAT		SYS	5	10
10.11.40.148	ORACLE	RUSHUAT		XMANINT	9	26
10.11.40.243	MYSQL		ASPNE	ASPNE	0	0
10.11.40.243	MYSQL		APP_MATRIX	APPNE	0	0
10.11.40.243	MYSQL		APP_MATRIX	MFREN	0	0
10.11.40.243	MYSQL		SIMPLE	MFREN	0	0

Records: 1 to 15 of 15

Aliases: OFF

Record Details

- 06 - Restrict DB user to certain IP
- Admin Users Sessions
- DB Predefined Users Sessions
- DB Server Throughput-Chart
- Detailed Sessions List

Guardium: Report Drilldown - Source: 01 - DB activities - Microsoft Internet Explorer

Back Forward Stop Home Favorites Print

**Guardium**

Server IP	Server Type	Service Name	Database Name	DB User Name	Sql	Total access
10.11.40.148	ORACLE	RUSHUAT		XMANINT	BEGIN DBMS_APPLICATION_INFO.SET_MODULE(1,NULL); END;	6
10.11.40.148	ORACLE	RUSHUAT		XMANINT	BEGIN DBMS_OUTPUT.DISABLE; END;	3
10.11.40.148	ORACLE	RUSHUAT		XMANINT	select * from nati	1
10.11.40.148	ORACLE	RUSHUAT		XMANINT	select * from tab1	1
10.11.40.148	ORACLE	RUSHUAT		XMANINT	SELECT ATTRIBUTE,SCOPE,NUMERIC_VALUE,CHAR_VALUE,DATE_VALUE FROM SYSTEM.PRODUCT_PRIVS WHERE (UPPER(?) LIKE UPPER(PRODUCT)) AND (UPPER (USER) LIKE USERID)	3
10.11.40.148	ORACLE	RUSHUAT		XMANINT	SELECT CHAR_VALUE FROM SYSTEM.PRODUCT_PRIVS WHERE (UPPER(?) LIKE UPPER(PRODUCT)) AND ((UPPER(USER) LIKE USERID) OR (USERID = ?)) AND (UPPER (ATTRIBUTE) = ?)	3
10.11.40.148	ORACLE	RUSHUAT		XMANINT	SELECT DECODE(?,?,?) FROM DUAL	3
10.11.40.148	ORACLE	RUSHUAT		XMANINT	select null from dual	3
10.11.40.148	ORACLE	RUSHUAT		XMANINT	SELECT USER FROM DUAL	3

Records: 1 to 9 of 9

# Admin User Sessions

Guardium (guardiumvm) - Microsoft Internet Explorer

Address: https://10.11.40.254:8443/sqlguard

10:38 [Edit Account: audit](#) [Customize](#) [Logout](#) [?](#)

G2000 - Standalone Unit

**View** | **Monitor/Audit** | **Discover** | **Assess/Harden** | **Comply** | **Protect**

**Overview** | **DB Activities** | **Exceptions** | **DB Administration** | **Schema Changes** | **Detailed Activities** | **Performance** | **Access Map** | **DB Entitlements**

Admin Users Login

- DB Predefined Users Login
- Administrative Commands Usage
- Administrative Objects Usage
- DML Execution on Administrative Objects
- BACKUP Commands Execution
- RESTORE Commands Execution
- REVOKE Commands Execution
- KILL Commands Execution
- DBCC Commands Execution
- GRANT Commands Execution

**Admin Users Sessions** Start Date: 2010-07-02 09:38:00 End Date: 2010-07-02 10:38:00

Client IP	DB User Name	Source Program	Session Start	Count of Sessions
10.11.40.13	SA	JAVA.EXE	2010-07-02 10:33:48.0	2
10.11.40.13	SA	JAVA.EXE	2010-07-02 10:34:03.0	2
10.11.40.13	SA	JAVA.EXE	2010-07-02 10:34:18.0	2
10.11.40.13	SA	JAVA.EXE	2010-07-02 10:34:32.0	1
10.11.40.13	SA	JAVA.EXE	2010-07-02 10:34:33.0	2
10.11.40.13	SA	JAVA.EXE	2010-07-02 10:34:48.0	2
10.11.40.13	SA	JAVA.EXE	2010-07-02 10:35:03.0	2
10.11.40.13	SA	JAVA.EXE	2010-07-02 10:35:18.0	2
10.11.40.13	SA	JAVA.EXE	2010-07-02 10:35:32.0	1
10.11.40.13	SA	JAVA.EXE	2010-07-02 10:35:33.0	2
10.11.40.13	SA	JAVA.EXE	2010-07-02 10:35:48.0	2
10.11.40.13	SA	JAVA.EXE	2010-07-02 10:36:03.0	2
10.11.40.13	SA	JAVA.EXE	2010-07-02 10:36:18.0	2
10.11.40.13	SYSTEM	JAVA.EXE	2010-07-02 10:36:32.0	1
10.11.40.13	SYSTEM	JAVA.EXE	2010-07-02 10:36:33.0	1
10.11.40.13	SYSTEM	JAVA.EXE	2010-07-02 10:36:34.0	1

Records: 301 to 316 of 316

Aliases: OFF

Guardium v7.0  
© Guardium 2002-2008

start | Document1 - Microsof... | Guardium (guardiumv... | Local intranet | 10:37 AM



# Execution of DDL Commands

Guardium (guardiumvm) - Microsoft Internet Explorer

Address: https://10.11.40.254:8443/sqlguard/media-type/html/user/audit/page/default.psm1/js\_pane/P-129219e12c0-10045

11:10 [Edit Account: audit](#) [Customize](#) [Logout](#)  
G2000 - Standalone Unit

**View** | **Monitor/Audit** | **Discover** | **Assess/Harden** | **Comply** | **Protect**

**Overview** | **DB Activities** | **Exceptions** | **DB Administration** | **Schema Changes** | **Detailed Activities** | **Performance** | **Access Map** | **DB Entitlements**

CREATE Commands Execution  
DDL Commands  
ALTER Commands Execution  
DDL Distribution  
DROP Commands Execution

**Execution Of DDL Commands**

Start Date: 2010-07-02 10:08:33 End Date: 2010-07-02 11:08:33

Client IP	Server IP	Server Type	SQL Verb	Count of Object Name	Total access
10.11.33.137	10.11.40.138	ORACLE	CREATE TRIGGER	10	14
10.11.40.138	10.11.40.138	ORACLE	CREATE TABLE	1	1
10.11.40.138	10.11.40.138	ORACLE	DROP TABLE	1	1

Records: 1 to 3 of 3

Aliases: OFF

Guardium v7.0  
© Guardium 2002-2008

start | PSBank.doc - Microso... | Guardium (guardiumv... | Guardium: Report Dril... | 10.11.40.138 - PUTTY | Local intranet | 11:10 AM

# Restrict DB Users to Certain IP Address

Guardium (guardiumvm) - Microsoft Internet Explorer

Address: https://10.11.40.254:8443/sqlguard/media-type/html/user/audit/page/default.psm/js\_pane/P-12989ef99a4-10008

11:22 Edit Account: audit Customize Logout G2000 - Standalone Unit

View Monitor/Audit Discover Assess/Harden Comply Protect

Build Audit Policies Build Reports My New Reports Privacy Sets POC

- 01 - DB activities
- 02 - correlate DB activity
- 03 - Separation of duties
- 04 - DBA activity
- 06 - Restrict DB user to certain IP
- 08 - Login Failed
- 09 - ILS\_USER\_NAMAD
- 10 - local access
- 11 - record affected
- 99 - ip list

**06 - Restrict DB user to certain IP**

Start Date: 2010-07-01 11:22:26 End Date: 2010-07-02 11:22:26

Timestamp	Access Rule Description	Client IP	DB User Name	Full SQL String	Count of Policy Rule Violations
2010-07-01 14:35:46.0	Restrict access by IP	10.11.40.138	POC_USER		1
2010-07-01 14:43:07.0	attached poc_user come from diff IP	10.11.40.138	POC_USER		1
2010-07-01 14:43:07.0	terminate poc_user come from diff IP	10.11.40.138	POC_USER		1
2010-07-01 14:43:24.0	terminate poc_user come from diff IP	10.11.40.138	POC_USER		1
2010-07-01 14:57:53.0	attached DBA	10.11.40.138	POC_USER		1
2010-07-01 14:58:52.0	Terminate CustomerID update	10.11.40.138	POC_USER		1
2010-07-01 15:26:43.0	alert on deviations	10.11.40.138	POC_USER	select * from customer where customerid=100	1
2010-07-01 15:28:17.0	alert on deviations	10.11.40.138	POC_USER	select customerid from customer	1
2010-07-01 17:30:26.0	attached DBA	10.11.40.138	POC_USER		1
2010-07-02 11:01:37.0	attached DBA	10.11.40.138	POC_USER		1
2010-07-02 11:02:02.0	attached DBA	10.11.40.138	POC_USER		1
2010-07-02 11:03:17.0	attached DBA	10.11.40.138	POC_USER		1

Records: 1 to 12 of 12

Aliases: OFF

Guardium v7.0  
© Guardium 2002-2008

start PSBank.doc - Microso... Guardium (guardiumv... 10.11.40.138 - PUTTY Local intranet 11:22 AM

# User Login Attempts

Guardium (guardiumvm) - Microsoft Internet Explorer

Address: https://10.11.40.254:8443/sqlguard/media-type/html/user/audit/page/default.psm1

Guardium 11:26 Edit Account: audit Customize Logout G2000 - Standalone Unit

View Monitor/Audit Discover Assess/Harden Comply Protect

Overview DB Activities Exceptions DB Administration Schema Changes Detailed Activities Performance Access Map DB Entitlements

Policy Violations  
Exceptions Distribution  
Exceptions Monitor  
Failed User Login Attempts  
SQL Errors  
Exception Count  
Terminated Users Logins  
Active Users Last Login  
Active Users with no Activity  
Terminated Users Failed Login Attempts

**Failed Login Attempts** Start Date: 2010-06-25 11:26:40 End Date: 2010-07-02 11:26:40

User Name	Source Address	Destination Address	Database Protocol	Count of Exceptions
	10.11.33.13	10.11.40.148	ORACLE	2
asdf	10.11.40.138	10.11.40.138	ORACLE	1
ils_manager	10.11.33.90	10.11.40.138	ORACLE	1
poc_user	10.11.40.138	10.11.40.138	ORACLE	2
SYS	10.11.40.148	10.11.40.148	ORACLE	3

Records: 1 to 5 of 5

Aliases: OFF

Guardium v7.0  
© Guardium 2002-2008

start PSBank.doc - Micro... Guardium (guardiumv... 10.11.40.138 - PUTTY Local intranet 11:26 AM

# Monitor Application Users

Guardium (guardiumvm) - Microsoft Internet Explorer

Address: https://10.11.40.254:8443/sqlguard/media-type/html/user/audit/page/default.psm/js\_pane/P-129219e12c0-10090

11:31 [Edit Account: audit](#) [Customize](#) [Logout](#) [G2000 - Standalone Unit](#)

**Guardium**

View Monitor/Audit Discover Assess/Harden Comply Protect

Build Audit Policies Build Reports My New Reports Privacy Sets POC

Custom Reporting

**Entity List**

- Client/Server
- Session
- Application Events
- FULL SQL Values
- FULL SQL
- SQL
- Access Period
- Command
- Object
- Object-Command
- Field
- Field SQL Value
- Object-Field

**09 - Monitor application users** Main Entity: Access Period  Sorted by occurrences

Query Fields							
Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend	
<input type="checkbox"/>	1	Access Period	Application User	Value		<input type="checkbox"/>	
<input type="checkbox"/>	2	FULL SQL	Full Sql	Value		<input type="checkbox"/>	
<input type="checkbox"/>	3	FULL SQL	Timestamp	Value		<input type="checkbox"/>	
<input type="checkbox"/>	4	Client/Server	Server IP	Value		<input type="checkbox"/>	
<input type="checkbox"/>	5	Client/Server	Service Name	Value		<input type="checkbox"/>	
<input type="checkbox"/>	6	Session	Database Name	Value		<input type="checkbox"/>	

Query Conditions				
Entity	Aggregate	Attribute	Operator	Runtime Param.

Back Remove Clone Roles... Save Done

Generate Tabular Add to My New Reports Generate and Add to...

Guardium v7.0  
© Guardium 2002-2008

Done Local intranet 11:31 AM

# Policy Violation Details

Guardium (guardiumvm) - Microsoft Internet Explorer

Address: https://10.11.40.254:8443/sqlguard/media-type/html/user/audit/page/default.psm1

11:46 [Edit Account](#) [audit](#) [Customize](#) [Logout](#) [?](#)

G2000 - Standalone Unit

**View** | **Monitor/Audit** | **Discover** | **Assess/Harden** | **Comply** | **Protect**

**Overview** | **DB Activities** | **Exceptions** | **DB Administration** | **Schema Changes** | **Detailed Activities** | **Performance** | **Access Map** | **DB Entitlements**

**Policy Violations**

- Exceptions Distribution
- Exceptions Monitor
- Failed User Login Attempts
- SQL Errors
- Exception Count
- Terminated Users Logins
- Active Users Last Login
- Active Users with no Activity
- Terminated Users Failed Login Attempts

**Policy Violations Details** Start Date: 2010-07-01 11:46:50 End Date: 2010-07-02 11:46:50

Timestamp	Category Name	Access Rule Description	Client IP	Server IP	DB User Name	Full SQL String	Severity	Count of Policy Rule Violations
2010-07-02 11:03:17.0		attached DBA	10.11.40.138	10.11.40.138	POC_USER		INFO	1
2010-07-02 11:02:02.0		attached DBA	10.11.40.138	10.11.40.138	POC_USER		INFO	1
2010-07-02 11:01:37.0		attached DBA	10.11.40.138	10.11.40.138	POC_USER		INFO	1
2010-07-01 23:15:39.0	after time hours work alert		10.11.40.243	10.11.40.243	MFRENDON	select count(*)as rCount from employee where (emp_hname like 'Flore %' or emp_fname like 'Flore %' or group_id like 'Flore %' or division like 'Flore %' or department like 'Flore %') and status='ENABLE'	MED	1
2010-07-01 23:15:39.0	after time hours work alert		10.11.40.243	10.11.40.243	MFRENDON	select emp_hname as LASTNAME,emp_fname as FIRSTNAME,direct_line as 'DIRECT LINE',fax_line as 'FAX LINE',local_line as 'LOCAL LINE',group_id as 'GROUP_DESC',division as 'DIVISION_AREA',department as 'DEPARTMENT_BRANCH' from employee where (emp_hname like 'Flore %' or emp_fname like 'Flore %' or group_id like 'Flore %' or division like 'Flore %' or department like 'Flore %') and status='ENABLE' order by LASTNAME ASC	MED	1
2010-07-01 23:15:39.0	after time hours work alert		10.11.40.243	10.11.40.243	MFRENDON	SET SQL_AUTO_JS_NULL=0;	MED	1
2010-07-01 23:15:39.0	after time hours work alert		10.11.40.243	10.11.40.243	MFRENDON	use app_matrix	MED	1
2010-07-01 23:15:38.0	after time hours work alert		10.11.40.243	10.11.40.243	MFRENDON	select count(*)as rCount from employee where (emp_hname like 'Flore %' or emp_fname like 'Flore %' or group_id like 'Flore %' or division like 'Flore %' or department like 'Flore %') and status='ENABLE'	MED	1
2010-07-01 23:15:38.0	after time hours work alert		10.11.40.243	10.11.40.243	MFRENDON	select emp_hname as LASTNAME,emp_fname as FIRSTNAME,direct_line as 'DIRECT LINE',fax_line as 'FAX LINE',local_line as 'LOCAL LINE',group_id as 'GROUP_DESC',division as 'DIVISION_AREA',department as 'DEPARTMENT_BRANCH' from employee where (emp_hname like 'Flore %' or emp_fname like 'Flore %' or group_id like 'Flore %' or division like 'Flore %' or department like 'Flore %') and status='ENABLE' order by LASTNAME ASC	MED	1
2010-07-01 23:15:38.0	after time hours work alert		10.11.40.243	10.11.40.243	MFRENDON	SET SQL_AUTO_JS_NULL=0;	MED	1
2010-07-01 23:15:38.0	after time hours work alert		10.11.40.243	10.11.40.243	MFRENDON	use app_matrix	MED	1
2010-07-01 23:15:34.0	after time hours work alert		10.11.40.243	10.11.40.243	MFRENDON	SELECT @@tx_isolation	MED	1
2010-07-01 23:15:34.0	after time hours work alert		10.11.40.243	10.11.40.243	MFRENDON	select count(*)as rCount from employee where (emp_hname like 'Flore %' or emp_fname like 'Flore %' or group_id like 'Flore %' or division like 'Flore %' or department like 'Flore %') and status='ENABLE'	MED	1
2010-07-01 23:15:34.0	after time hours work alert		10.11.40.243	10.11.40.243	MFRENDON	select database()	MED	1
2010-07-01 23:15:34.0	after time hours work alert		10.11.40.243	10.11.40.243	MFRENDON	select emp_hname as LASTNAME,emp_fname as FIRSTNAME,direct_line as 'DIRECT LINE',fax_line as 'FAX LINE',local_line as 'LOCAL LINE',group_id as 'GROUP_DESC',division as 'DIVISION_AREA',department as 'DEPARTMENT_BRANCH' from employee where (emp_hname like 'Flore %' or emp_fname like 'Flore %' or group_id like 'Flore %' or division like 'Flore %' or department like 'Flore %') and status='ENABLE' order by LASTNAME ASC	MED	1
2010-07-01 23:15:34.0	after time hours work alert		10.11.40.243	10.11.40.243	MFRENDON	SET SQL_AUTO_JS_NULL=0;	MED	2
2010-07-01 23:10:03.0	after time hours work alert		10.11.40.243	10.11.40.243	MFRENDON	select count(*)as rCount from employee where (emp_hname like 'Flore Micah%' or emp_fname like 'Flore Micah%' or group_id like 'Flore Micah%' or division like 'Flore Micah%' or department like 'Flore Micah%') and status='ENABLE'	MED	1

start | PSBank.doc - Microso... | Guardium (guardiumv... | 10.11.40.138 - PUTTY | Local intranet | 11:46 AM

# Database Servers Monitored

Guardium (guardiumvm) - Microsoft Internet Explorer

Address: https://10.11.40.254:8443/sqlguard/media-type/html/user/audit/page/default.psm1/js\_pane/P-129219e12c0-10012

13:11 [Edit Account: audit](#) [Customize](#) [Logout](#) [G2000 - Standalone Unit](#)

**Guardium**

View Monitor/Audit Discover Assess/Harden Comply Protect

Overview DB Activities Exceptions DB Administration Schema Changes Detailed Activities Performance Access Map DB Entitlements

Sessions By Server Type  
 DML Execution on Sensitive Objects  
 Sensitive Objects Usage  
 Activity By Client IP  
 Database Servers

**Servers Accessed**

Start Date: 2010-07-01 13:11:09 End Date: 2010-07-03 13:11:09

Server IP	Server Type	Database Name	Service Name	Count of Source Program	Count of Sessions
10.11.40.13	MS SQL SERVER			1	5
10.11.40.13	MS SQL SERVER	SDMSUAT		2	12976
10.11.40.138	ORACLE		ILSPROD	11	100
10.11.40.138	ORACLE		ORACLEILSPROD	1	11
10.11.40.138	ORACLE		ORACLEILSTEST	1	3
10.11.40.148	ORACLE			1	2
10.11.40.148	ORACLE		RUSHUAT	1	9
10.11.40.243	MYSQL			1	1
10.11.40.243	MYSQL	APP_MATRIX		1	2698
10.11.40.243	MYSQL	SIMPLE		2	44

Records: 1 to 10 of 10

Aliases: OFF

**Databases Discovered**

No data found for requested query

Guardium v7.0  
 © Guardium 2002-2008

start PSBank.doc - Microso... Guardium (guardiumv... 10.11.40.138 - PuTTY 10.11.40.148 - Remo... Local intranet 1:10 PM

# S-TAP Status

Guardium Admin Console (guardiumvm) - Microsoft Internet Explorer

Address: https://10.11.40.254:8443/sqlguard/media-type/html/user/admin/page/default.psm/js\_pane/P-10f960c7b25-10001

11:52 Edit Account: admin Customize Logout G2000 - Standalone Unit

System View Administration Console Tools Daily Monitor Guardium Monitor Tap Monitor Incident Management

S-Tap CAS

Rogue Connections  
S-Tap Configuration Change History  
Primary Guardium Host Change Log  
STAP Status  
Inactive STAPs Since

S-Tap Host	S-Tap Version	DB Server Type	Status	Last Response	Primary Host Name	KTAP Installed	TEE Installed	Shared Memory Driver Installed	DB2 Shared Memory Driver Installed	LHMON Driver Installed	Named Pipes Driver Installed	Hunter DBS	App Server Installed	Encrypted?
10.11.40.13	7.0.1.38	MSSQL	Active	2010-07-02 11:52:45.0	10.11.40.254	No	No	Yes	No	Yes	Yes		No	Unencrypted
10.11.40.138	STAP-7.0.0-20091203-1344	ORACLE	Active	2010-07-02 11:52:44.0	10.11.40.254	Yes	No	No	No	No	No	NULL	No	Unencrypted
10.11.40.148	7.0.1.38	ORACLE	Inactive	2010-07-02 11:49:45.0	10.11.40.254	No	No	No	No	Yes	Yes		No	Unencrypted
10.11.40.243	7.0.1.38	MYSQL	Active	2010-07-02 11:52:45.0	10.11.40.254	No	No	No	No	Yes	No		No	Unencrypted
10.11.40.83	7.0.1.38	DB2	Active	2010-07-02 11:52:45.0	10.11.40.254	No	No	No	Yes	Yes	No		No	Unencrypted

Records: 1 to 5 of 5

Aliases: OFF

Guardium v7.0  
© Guardium 2002-2008

start PSBank.doc - Microso... Guardium Admin Cons... 10.11.40.138 - PuTTY 10.11.40.148 - Remo... Local intranet 11:52 AM

# Vulnerability Assessment Example

**Guardium**
?

Results for Security Assessment: **Comprehensive Oracle Assessment** -- Select another result --

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%**

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](#)

**Assessment Result History**

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



## 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



# The *Continuing* Choice of Telco/Utility Market Leaders


# The *Continuing* Choice of Financial Market Leaders


**Guardium**<sup>®</sup>  
 SAFEGUARDING DATABASES™ | AN IBM® COMPANY

# The *Continuing* Choice of Oil and Gas Leaders


# The *Continuing* Choice of Government Leaders


# Validated by Industry Experts



*"Dominance in this space"*  
#1 Scores for Current Offering,  
Architecture & Product Strategy



**"Most Powerful  
Compliance Regulations"**



*"5-Star Ratings: Easy  
installation, sophisticated  
reporting, strong policy-  
based security."*



**"Guardium is ahead of the  
pack and gaining  
speed."**



*"Top of DBEP Class"*

*"Practically every feature you'll  
need to get down to business with  
data..."*

**speed."**



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



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



**Guardium®**

SAFEGUARDING DATABASES™ | AN IBM® COMPANY



# Guardium Value Proposition

- **Ensure privacy & integrity of enterprise data**
  - Enforce change controls & access controls for critical systems
  - Across entire application & database infrastructure
  - Oracle, SQL Server, IBM DB2 & Informix, Sybase, MySQL, Teradata
  - SAP, Oracle Financials, PeopleSoft, Siebel, Business Objects, ...
- **Increase operational efficiency**
  - Automate & centralize internal controls
  - Across heterogeneous & distributed environments
  - Rapidly troubleshoot performance issues & application errors
  - Highly-scalable platform proven in most demanding data center environments worldwide
- **No degradation of infrastructure or business processes**
  - Non-invasive architecture
  - No changes required to applications or databases

## Summary & Conclusions

- Databases contain your most critical data
- Traditional technologies can't give you the visibility to identify & prevent unauthorized access
- Guardium is the most widely-deployed solution
  - Broad heterogeneous support
  - Granular visibility & real-time policies
  - Deep automation
  - Scalable architecture



# General Discussion



Thank  
YOU



# Customer Case Studies

## 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 & 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

# 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.

# 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.”



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.”





## Why Enterprises Choose Guardium

- Most widely-deployed in production environments
  - *Continuously enhanced since 2002, based on real-world enterprise feedback*
- Most scalable & automated solution (enterprise-ready)
  - *Federated multi-tier system with centralized, cross-DBMS security policies and audit repository, groups, auto-discovery, compliance workflow automation, incident management, role-based management, ...*
- Most flexible
  - *Multiple deployment options, configurable policies, drag-and-drop reporting, API, ...*
- Broadest support for heterogeneous environments
  - *Database & OS platforms, enterprise applications, authentication, data import, integration with SIEM & ticketing systems,*
- Richest suite of security & compliance applications
  - *Security & forensics, compliance reporting & oversight, change control, data mining, log data management, ...*

# Supported Platforms

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