The State of Database Security:
The Case for Database Activity Monitoring

Scott Henley – IBM WW Security Tiger Team
scott.henley@au1.ibm.com

PulseANZ 2010

Meet the people who can help advance your infrastructure

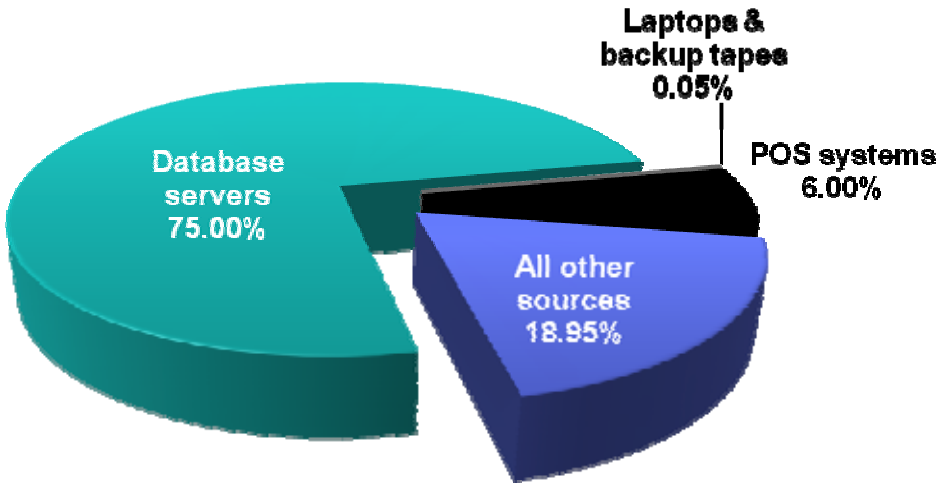
Trademarks and disclaimers

Agenda

- The State of Database Security
- Analyst report on top 10 database monitoring requirements
- Current state of database activity monitoring
- Alternate Approach to Securing Sensitive Data
- Addressing the top 10 requirements

Database Servers Are The Primary Source of Breached Data

% of Record Breached (2009)



"73% of security professionals anticipate the volume of database security attacks will continue to increase"

- Enterprise Strategy Group, Databases at Risk, September 2009

Breach Report from Verizon Business RISK Team

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

Why?

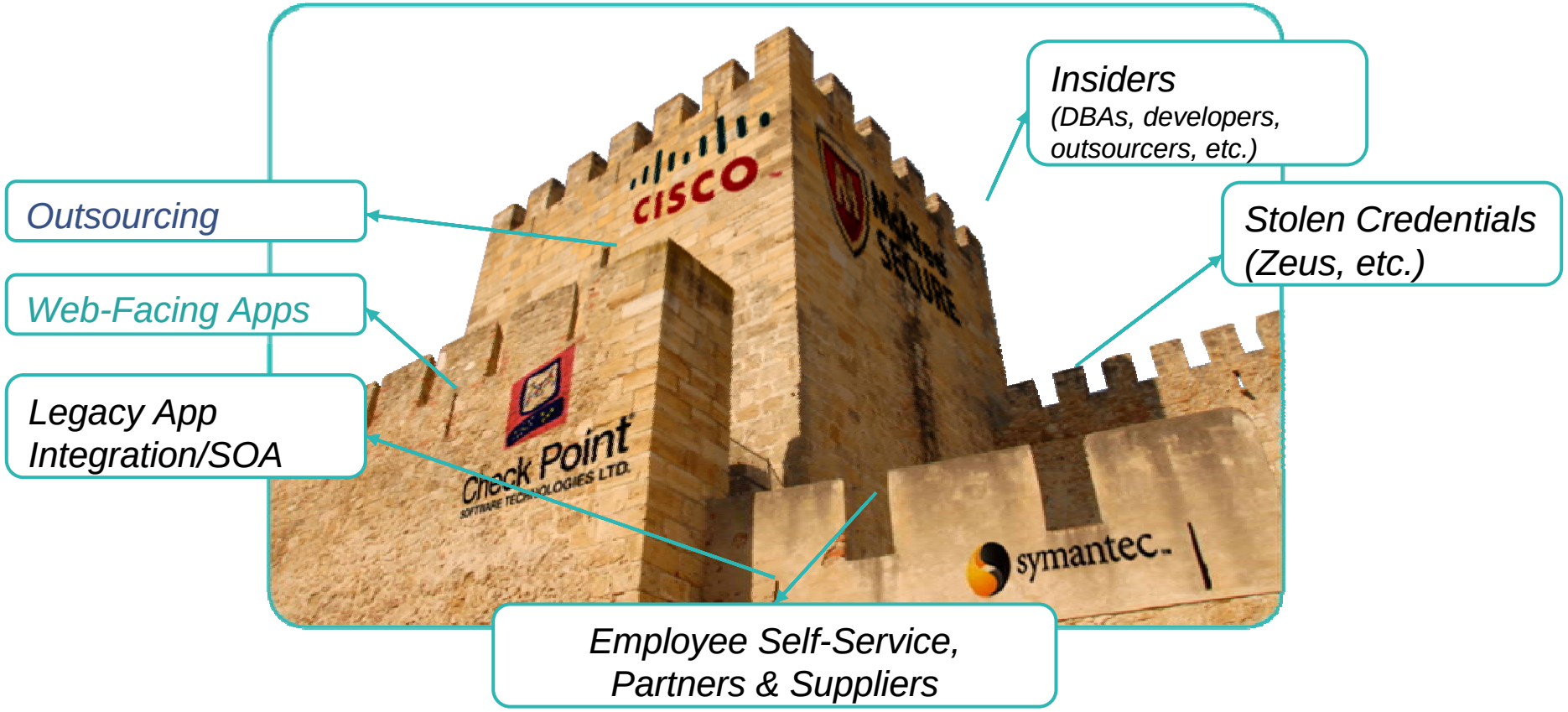
- Database servers contain your most valuable information
  - Financial records
  - Customer information
  - Credit card and other account records
  - Personally identifiable information
- High volumes of structured data
- Easy to access

"Because that's where the money is."
- **Willie Sutton**

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



Gartner* “Most enterprises are paying too little attention to the very real security risks associated with their databases.”

Key Findings:

- The use of **structured data storage**, and the amount of data stored in this way, are **increasing rapidly**. This trend is largely driven by data analytics requirements and consolidation efforts.
- The **information** stored in enterprise databases is **increasingly sensitive** and subject to legal, regulatory and other compliance requirements.
- Despite the growing criticality of their databases, **many enterprises continue to rely heavily on inadequate network and application-layer controls**, and perform only minimal monitoring on database storage infrastructure.

Recommendations:

- Evaluate your enterprise's current database controls to **identify gaps** and implement compensating or **mitigating controls** for those gaps.
- **Identify the monitoring use cases** that apply to your enterprise's database infrastructure, and **deploy tools to support those use cases** effectively and efficiently.
- Develop and communicate a clear policy specifying what database-related **behaviors should be audited** and why.
- Conduct a **database risk assessment**, applying a balanced approach to risk management and mitigation based on risk, criticality, and regulatory and other compliance requirements.

Gartner research ID Number: G00200212 “Ten Database Activities Enterprises Need to Monitor” - Published April 2010

Ten Database Activities that Enterprises Need to Monitor

Privileged Users:
1. Access to, deletion of or changes to data.
2. Access using inappropriate or non-approved channels.
3. Schema modifications.
4. Unauthorised additions or modifications of accounts.

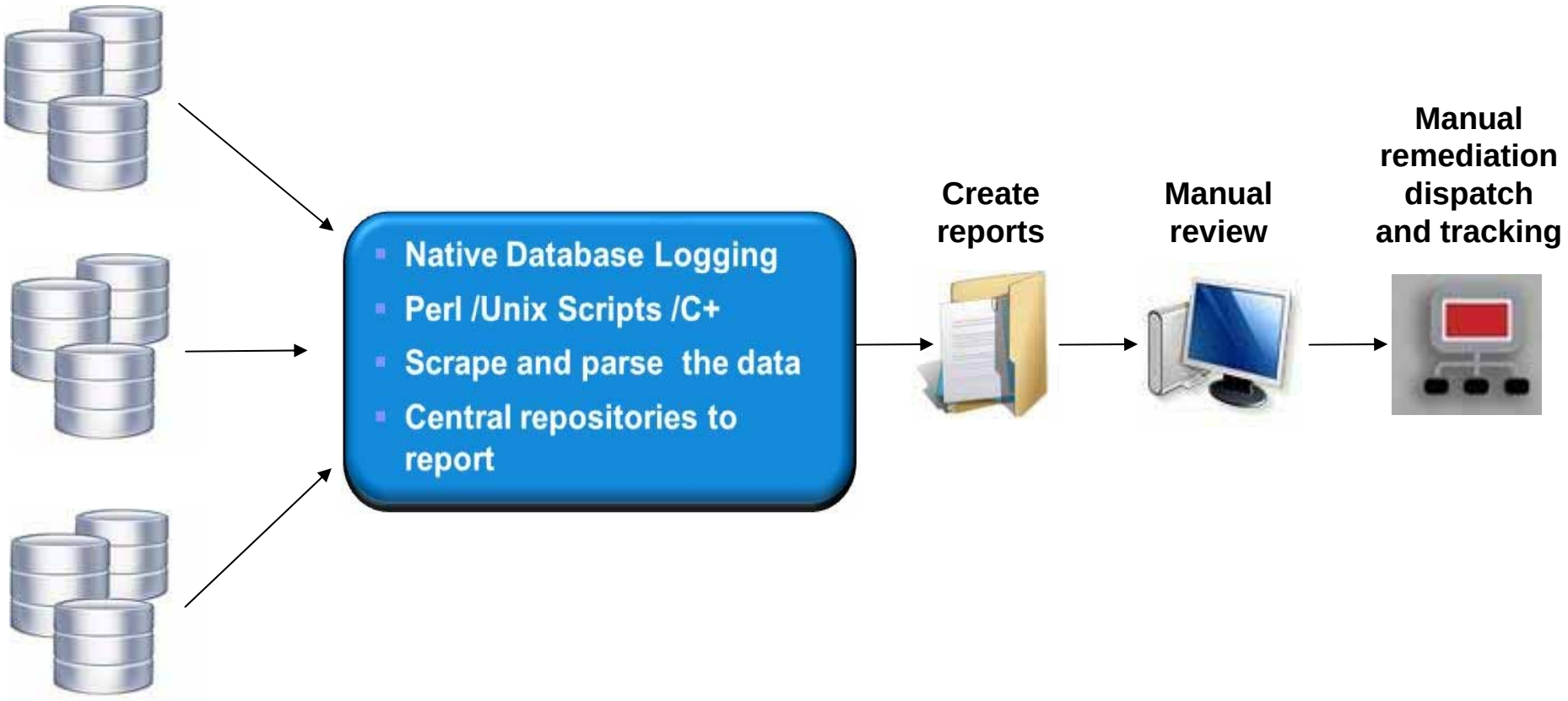
End Users:
5. Access to excessive amounts of data or data not needed for legitimate work.
6. Access to data outside standard working hours.
7. Access to data through inappropriate or non-approved channels.

Developers, System Analysts and System Administrators:
8. Access to live production systems.

IT Operations:
9. Unapproved changes to databases or applications that access the database.
10. Out-of-cycle patching of production systems.

Gartner research ID Number: G00200212 “Ten Database Activities Enterprises Need to Monitor”, Jeffrey Wheatman, 28 April 2010

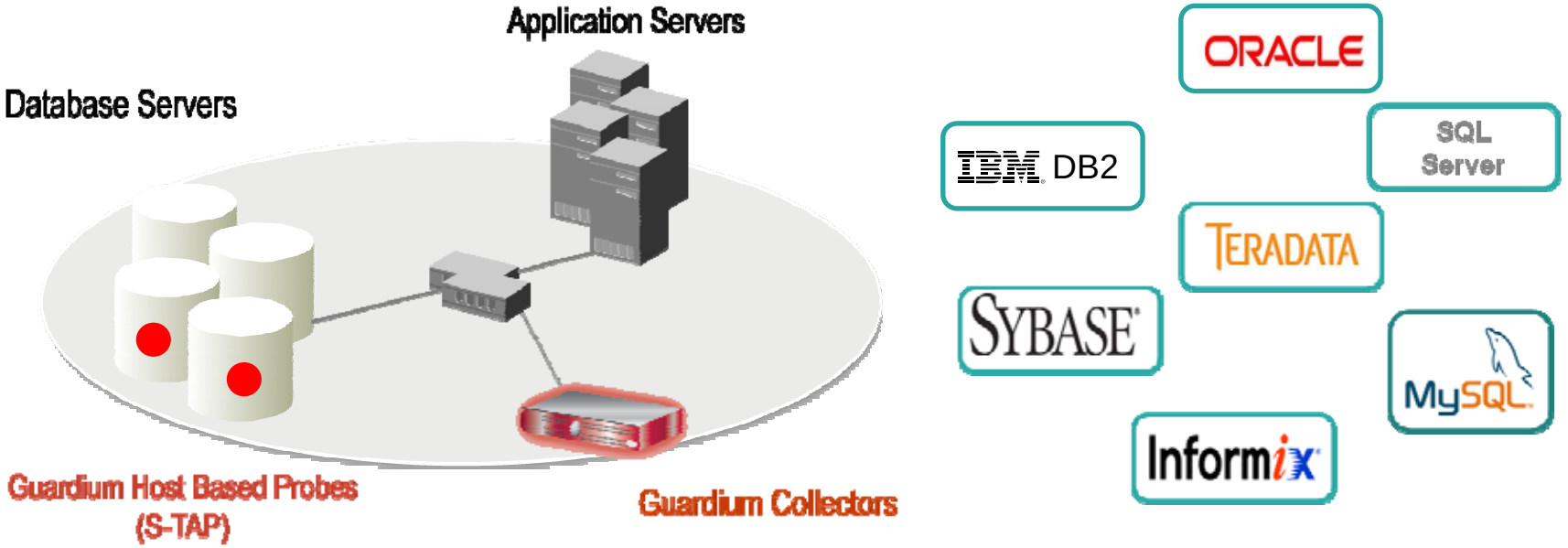
What Database Audit Tools are Enterprises Using Today?



What Are the Challenges?

- No separation of duties; DBA run the process
- Performance impact of native logging on the DBMS
- Limited scope of logging data
- Not real-time
- Significant labor cost to review data and maintain process
- Another data store to secure and manage
- Manual remediation is error prone and costly
- Poor audit trail
- Inconsistent policies across systems and business units
- Lack of DBMS expertise

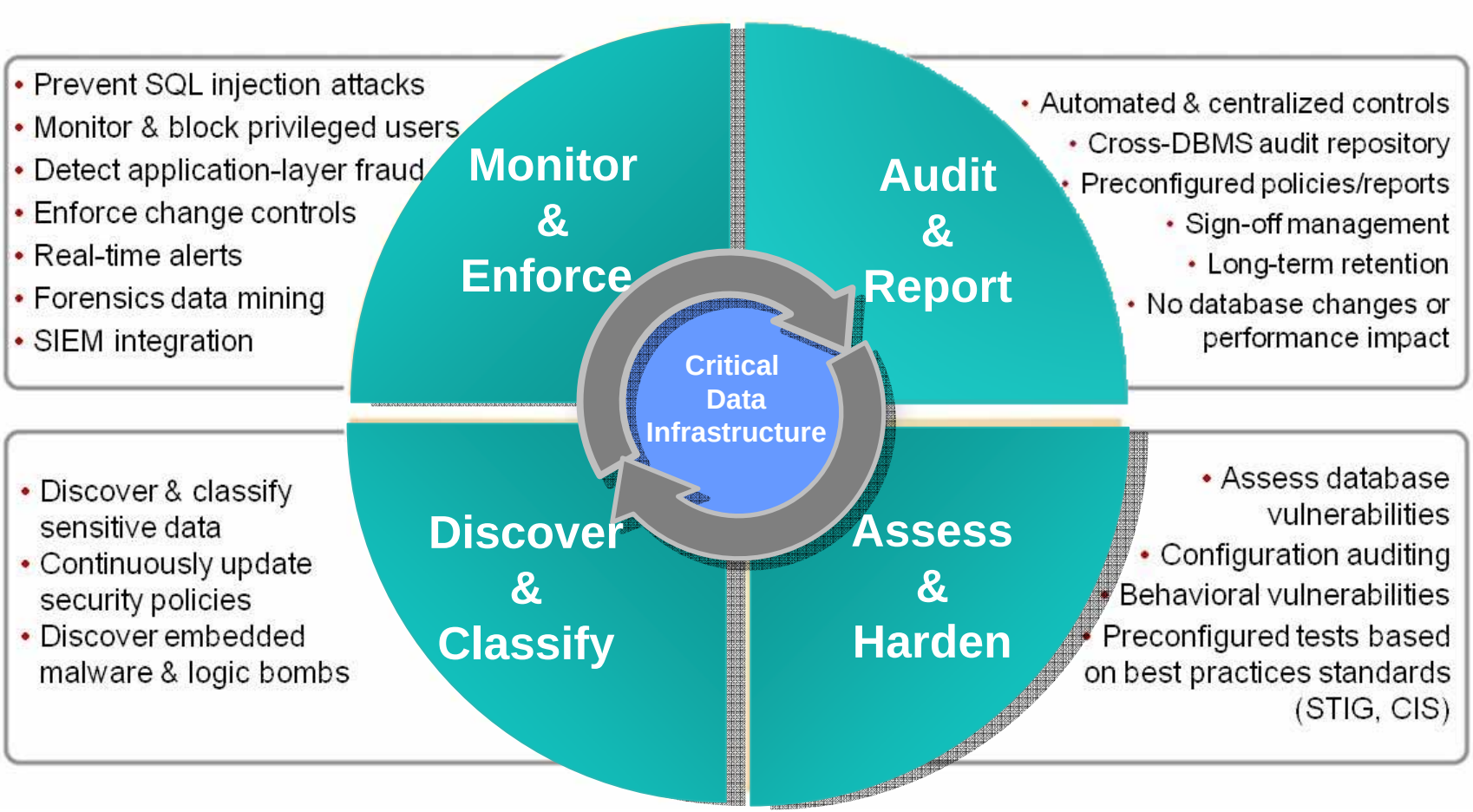
Database Activity Monitoring (DAM): An Alternate Approach to Securing Sensitive Data



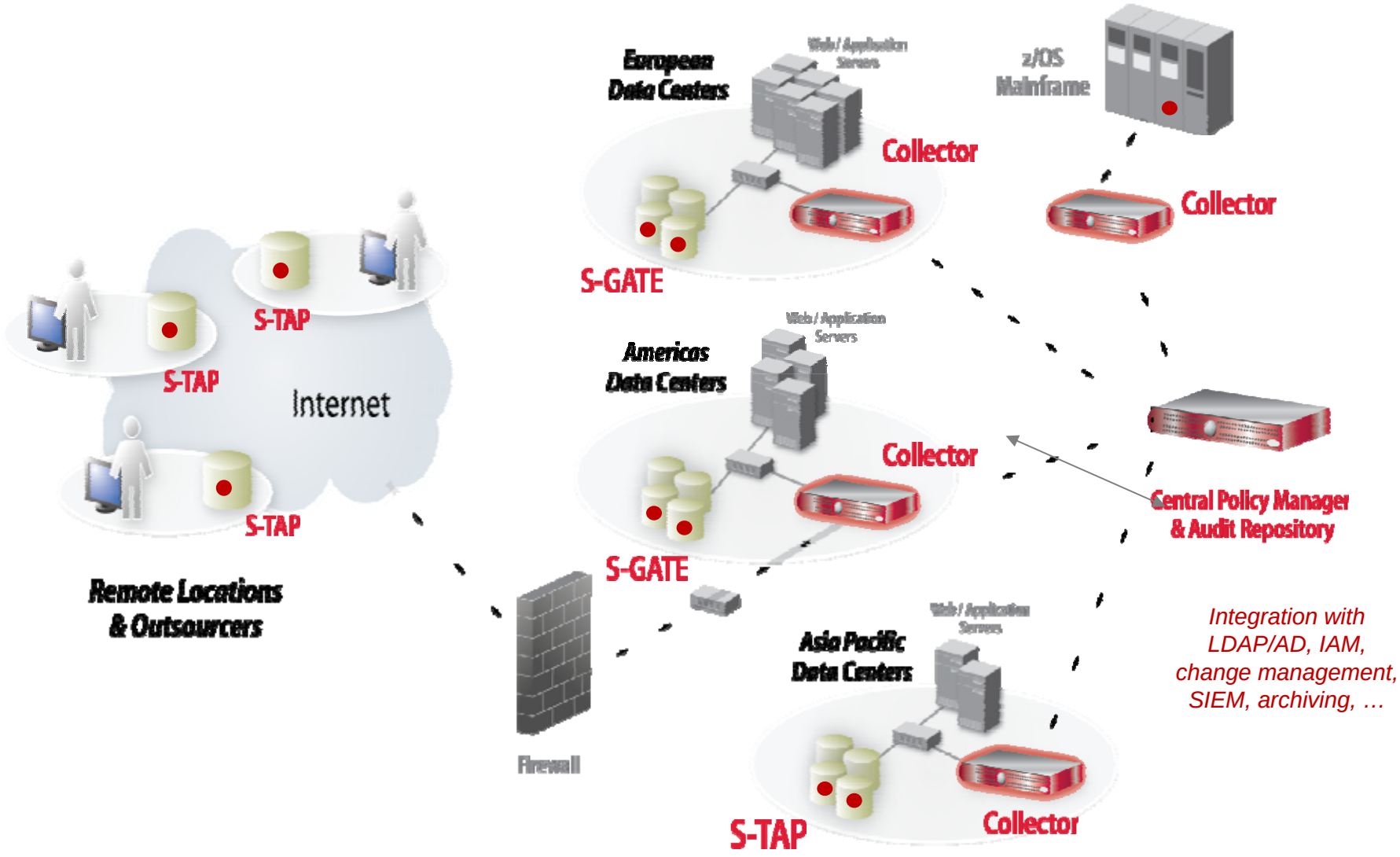
- Non-invasive architecture
  - Outside database
  - Minimal performance impact (2-3%)
  - No DBMS or application changes
- Cross-DBMS solution (some vendors)
- 100% visibility including local DBA access
- Enforces separation of duties (SoD)
- Does not rely on DBMS-resident logs that can easily be erased by attackers, rogue insiders
- Granular, real-time policies & auditing
  - *Who, what, when, how*
- Automated compliance reporting, sign-offs & escalations (SOX, PCI, NIST, etc.)

A different approach – Guardium

Able to Address the Full Database Security Lifecycle



Scalable Enterprise-Wide Architecture

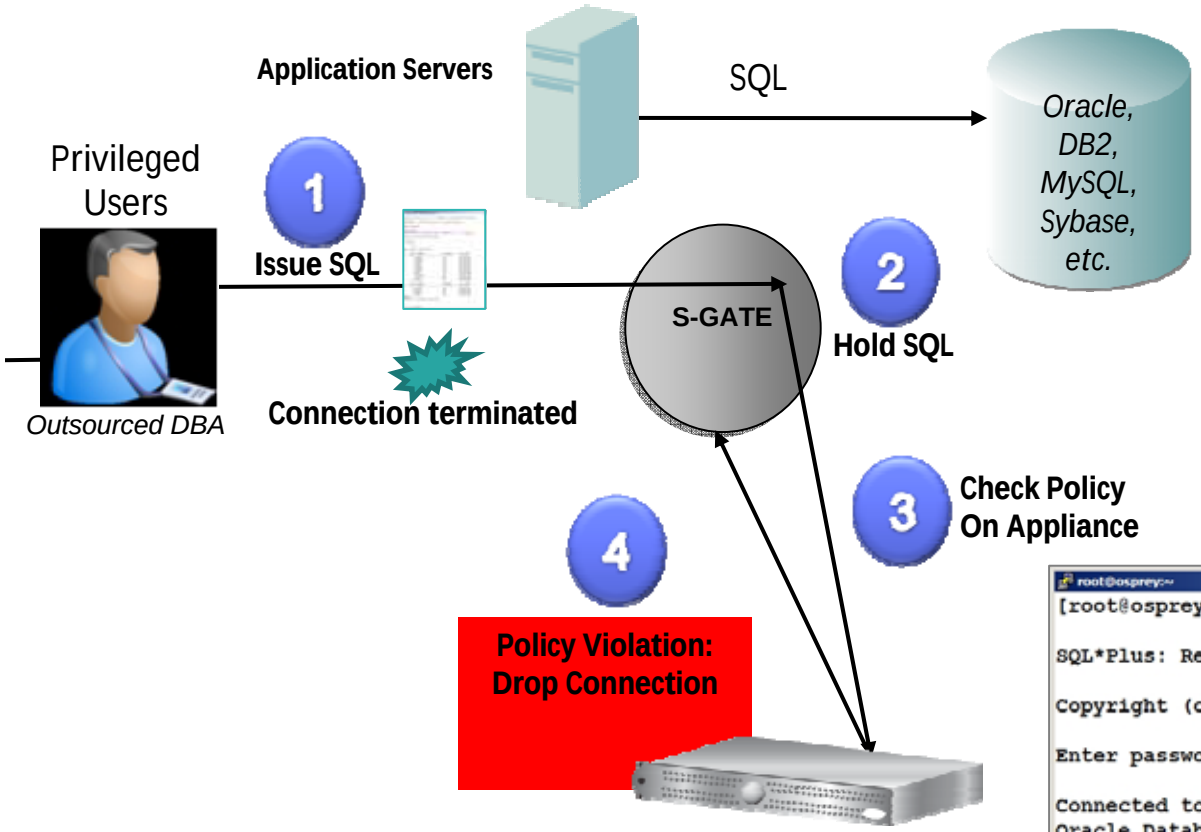


Integration with LDAP/AD, IAM, change management, SIEM, archiving, …

Privileged Users

Privileged Users	Access or changes to data
	Access via inappropriate or unapproved channels
	Schema modifications
	Addition or modification of accounts

Privileged Users Prevented From Accessing Sensitive Information Cross-DBMS, Data-Level Access Control (S-GATE)



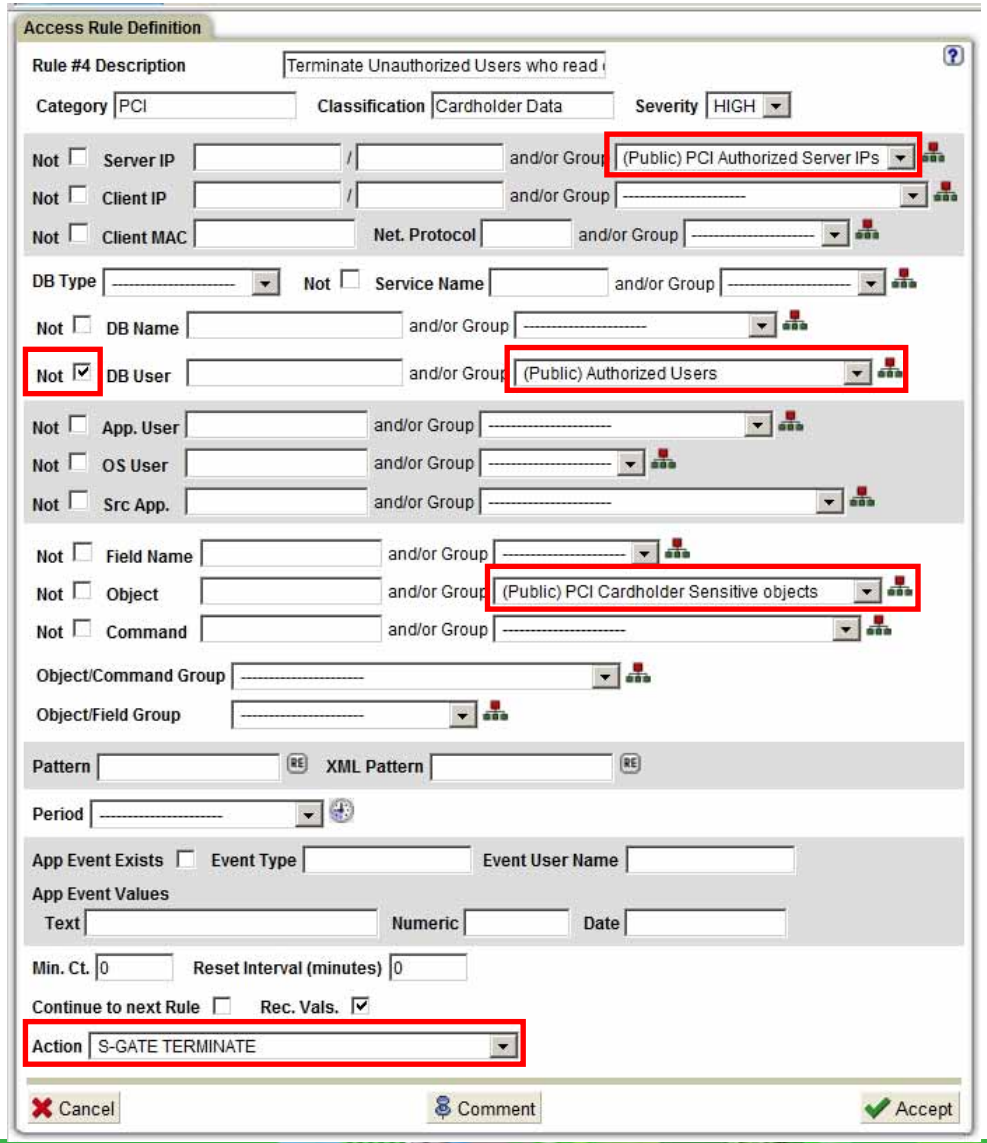
- ✓ Cross-DBMS policies
- ✓ Block privileged user actions
- ✓ No database changes
- ✓ No application changes
- ✓ Without risk of inline appliances that can interfere with application traffic

Privileged Users	
	Access or changes to data
	Access via inappropriate or unapproved channels
	Schema modifications
	Addition or modification of accounts

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

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

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

Enter password:

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

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

SQL>
```

Session Terminated

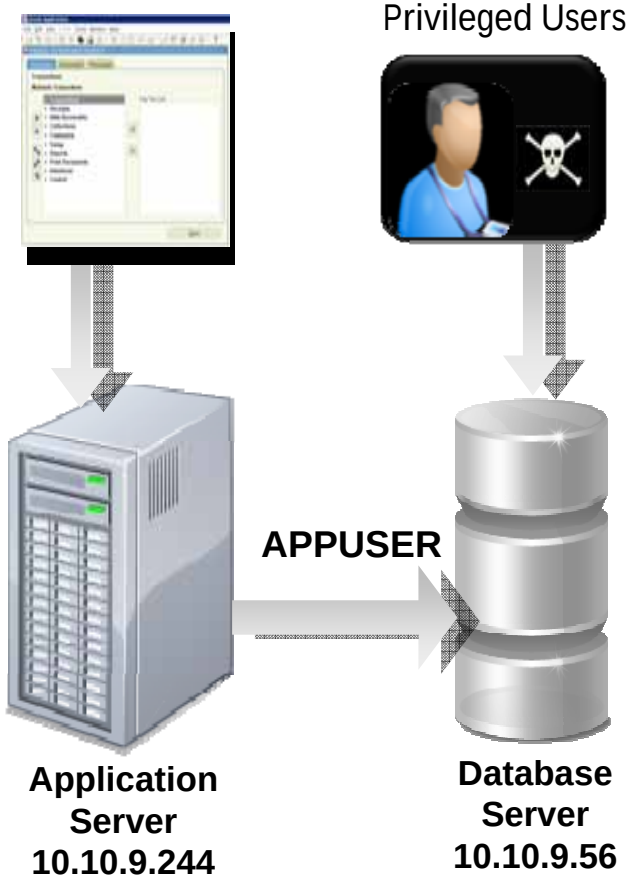
DBMS-Independent Auditing & Access Control Policy

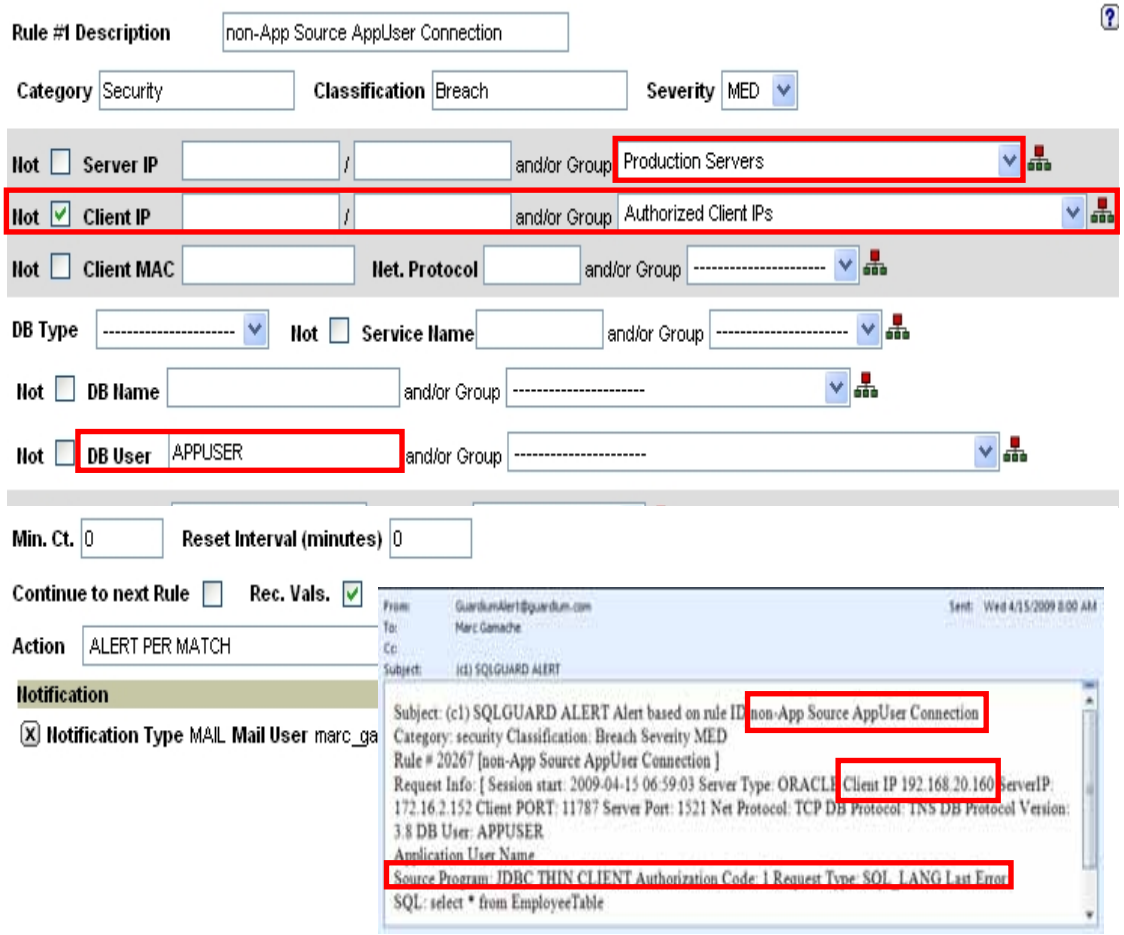


- PCI Servers
- Everyone that is NOT an authorized user
- Access PCI Sensitive Objects
- Will be terminated

Guardium
SAFEGUARDING DATABASES | AN IBM COMPANY

Privileged Users – Inappropriate and Unapproved Channels





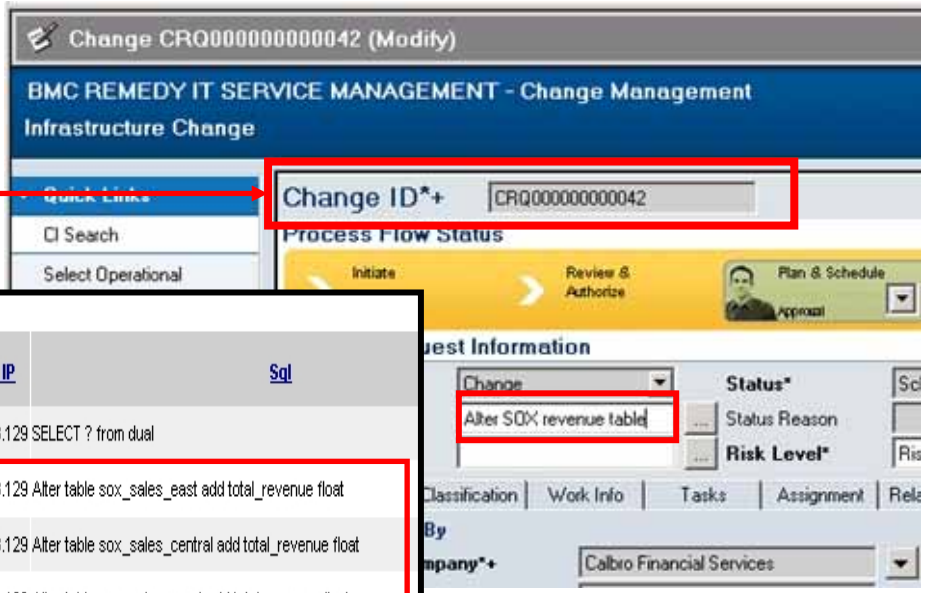
Privileged Users	Access or changes to data
	Access via inappropriate or unapproved channels
	Schema modifications
	Addition or modification of accounts

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

Guardium
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

Privileged Users – Schema Modification

Guardium unifies change management process for databases



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	change_id_entered	Assigned To	DB User Name	Client IP	Server IP	Sql
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

Privileged Users	Access or changes to data
	Access via inappropriate or unapproved channels
	Schema modifications
	Addition or modification of accounts

Guardium
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

Privileged Users – Modification of Accounts (Oracle EBS Example)

EBS Application Access

Start Date: 2009-02-20 14:49:48 End Date: 2009-02-20 16:49:48

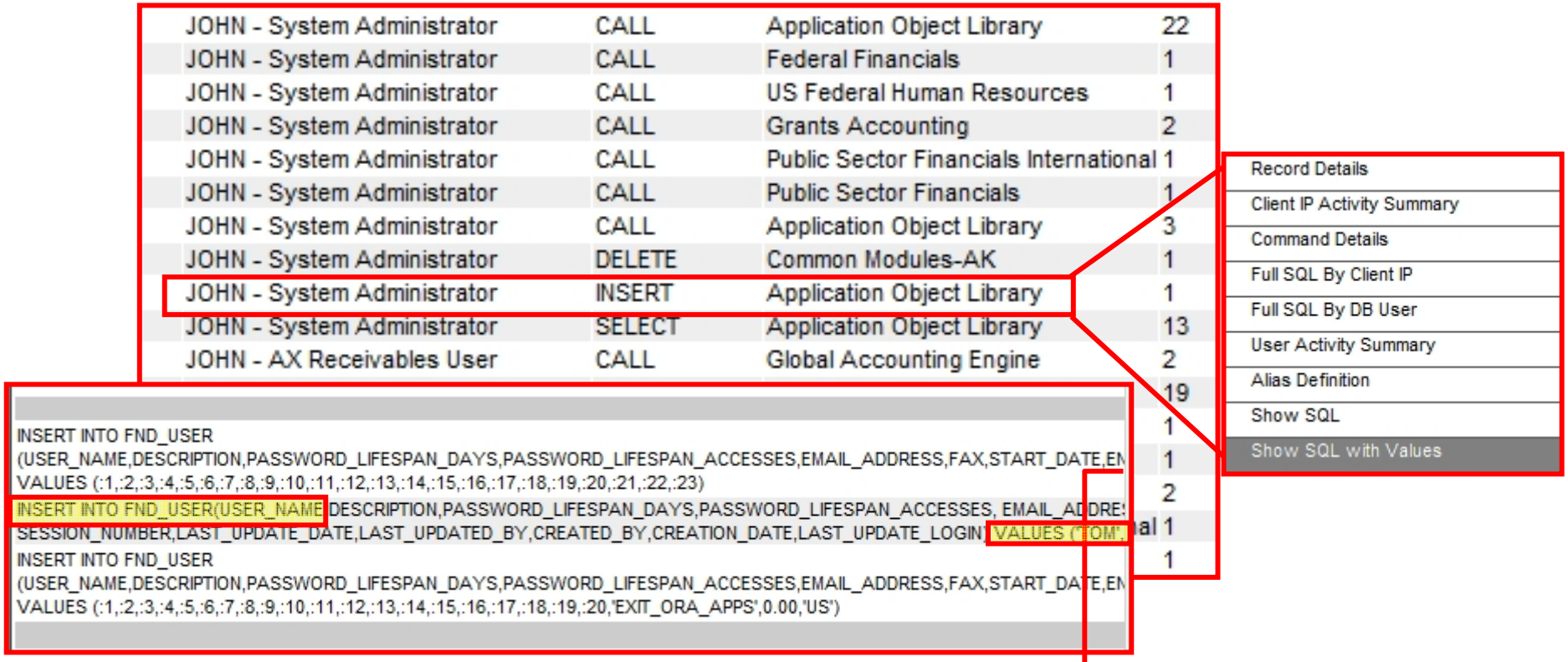
P					Name
2009-	JOHN - System Administrator	CALL	Application Object Library	22	
2009-	JOHN - System Administrator	CALL	Federal Financials	1	
2009-	JOHN - System Administrator	CALL	US Federal Human Resources	1	
2009-	JOHN - System Administrator	CALL	Grants Accounting	2	
2009-	JOHN - System Administrator	CALL	Public Sector Financials International	1	
2009-	JOHN - System Administrator	CALL	Public Sector Financials	1	
2009-	JOHN - System Administrator	CALL	Application Object Library	3	
2009-	JOHN - System Administrator	DELETE	Common Modules-AK	1	
2009-	JOHN - System Administrator	INSERT	Application Object Library	1	
2009-	JOHN - System Administrator	SELECT	Application Object Library	13	
2009-	JOHN - AX Receivables User	CALL	Global Accounting Engine	2	
2009-	JOHN - AX Receivables User	CALL	Application Object Library	19	
2009-	JOHN - AX Receivables User	CALL	Federal Financials	1	
2009-	JOHN - AX Receivables User	CALL	US Federal Human Resources	1	
2009-	JOHN - AX Receivables User	CALL	Grants Accounting	2	
2009-	JOHN - AX Receivables User	CALL	Public Sector Financials International	1	
2009-	JOHN - AX Receivables User	CALL	Public Sector Financials	1	
2009-02-20 16:00:00.0	192.168.2.148 APPS	BOB - AX General Ledger Supervisor	CALL	Public Sector Financials International	1
2009-02-20 16:00:00.0	192.168.2.148 APPS	BOB - AX General Ledger Supervisor	CALL	Public Sector Financials	1
2009-02-20 16:00:00.0	192.168.2.148 APPS	BOB - AX General Ledger Supervisor	CALL	Application Object Library	4
2009-02-20 16:00:00.0	192.168.2.148 APPS	BOB - AX General Ledger Supervisor	SELECT	Global Accounting Engine	1
2009-02-20 16:00:00.0	192.168.2.148 APPS	BOB - AX General Ledger Supervisor	SELECT	Application Object Library	24
2009-02-20 16:00:00.0	192.168.2.148 APPS	JOHN - System Administrator	CALL	Application Object Library	22
2009-02-20 16:00:00.0	192.168.2.148 APPS	JOHN - System Administrator	CALL	Federal Financials	1
2009-02-20 16:00:00.0	192.168.2.148 APPS	JOHN - System Administrator	CALL	US Federal Human Resources	1
2009-02-20 16:00:00.0	192.168.2.148 APPS	JOHN - System Administrator	CALL	Grants Accounting	2
2009-02-20 16:00:00.0	192.168.2.148 APPS	JOHN - System Administrator	CALL	Public Sector Financials International	1
2009-02-20 16:00:00.0	192.168.2.148 APPS	JOHN - System Administrator	CALL	Public Sector Financials	1
2009-02-20 16:00:00.0	192.168.2.148 APPS	JOHN - System Administrator	CALL	Application Object Library	3
2009-02-20 16:00:00.0	192.168.2.148 APPS	JOHN - System Administrator	DELETE	Common Modules-AK	1
2009-02-20 16:00:00.0	192.168.2.148 APPS	JOHN - System Administrator	INSERT	Application Object Library	1
		JOHN - System Administrator	SELECT	Application Object Library	13
		JOHN - AX Receivables User	CALL	Global Accounting Engine	2
		JOHN - AX Receivables User	CALL	Application Object Library	19
		JOHN - AX Receivables User	CALL	Federal Financials	1
		JOHN - AX Receivables User	CALL	US Federal Human Resources	1
		JOHN - AX Receivables User	CALL	Grants Accounting	2
		JOHN - AX Receivables User	CALL	Public Sector Financials International	1
		JOHN - AX Receivables User	CALL	Public Sector Financials	1

Two Roles?

Privileged Users	
	Access or changes to data
	Access via inappropriate or unapproved channels
	Schema modifications
	Addition or modification of accounts

Guardium
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

Monitoring System Administration Roles



- Why is John the System Administrator, and the AX Receivables Role?

- Why did John add the user Tom?

Guardium
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

End Users

End Users	Access to excessive or unneeded data
	Data access outside standard hours
	Access via inappropriate or nonapproved channels

Access To Excessive or Unneeded Data

Should my customer service rep view 99 records in an hour when average is 4?

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

Is this normal?

What did he see?

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

End Users	Access to excessive or unneeded data
	Data access outside standard hours
	Access via inappropriate or nonapproved channels

Guardium
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

After-Hours Changes

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

Timestamp	Server Type	DB User Name	Client IP	Server IP	Sql
2009-01-24 5:14:19.0	ORACLE	RAJ	192.168.8.129	192.168.8.129	insert into alen.scz_sales_east (customer,zipcode,revenue,total_revenue,sum_total) values(?,?,?,?,?)

Time Period

	Time Period Description	Hour From	Hour To	Weekday From	Weekday To	Contiguous
☐	7x24	00:00	24:00	Sunday	Saturday	☑
☐	AFTER HOURS WORK	18:00	24:00	Monday	Friday	☐
☐	BEFORE HOURS WORK	00:00	08:00	Monday	Friday	☐
☐	EVENING	18:00	24:00	Monday	Friday	☐
☐	REGULAR WORK DAY	08:00	18:00	Monday	Friday	☐
☐	SATURDAY	00:00	24:00	Saturday	Saturday	☐
☐	SUNDAY	00:00	24:00	Sunday	Sunday	☐
☐	WEEK END	18:00	08:00	Friday	Monday	☑

Cancel | Select All | Unselect All | Remove

Time Period Description: Custom Time Period Contiguous ☑

Hour From: 17:00 Hour To: 05:00

Weekday From: Friday Weekday To: Monday

Add

Access Rule Definition

Rule #2 Description: Alert on after hours changes

Category: Data Security Classification: Unauthorized Changes Severity: HIGH

Not ☐ Field Name and/or Group

Not ☐ Object and/or Group

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

Object/Command Group

Object/Field Group

Pattern XML Pattern

Period: AFTER HOURS WORK

App Event Exists ☐ Event Type Event User Name

App Event Values

Text Numeric Date

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

Continue to next Rule ☑ Rec. Vals. ☑

Action: ALERT PER MATCH

Notification

☒ Notification Type SYSLOG Alert Receiver SYSLOG

End Users	Access to excessive or unneeded data
	Data access outside standard hours
	Access via inappropriate or nonapproved channels

Guardium® SAFEGUARDING DATABASES™ | AN IBM® COMPANY

End User - Access via non-approved channels

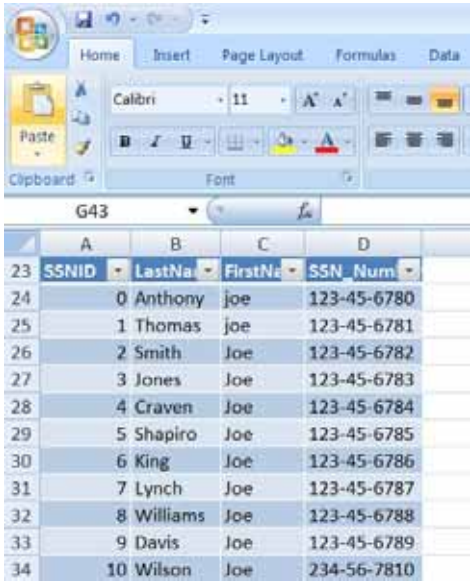
- User accessing database via Microsoft Office

- SQL Trace with Session ID

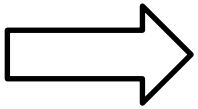
Start Date: **2010-06-18 13:41:57** End Date: **2010-06-18 17:41:57**
Aliases: **OFF** FULLSQL: **LIKE %ssn%**

Timestamp	Client IP	Server IP	DB User Name	Source Program	Full Sql	Succeeded
2010-06-18 16:30:44.0	10.10.9.240	10.10.9.251	SA	2007 MICROSOFT OFFICE SYSTEM	select * from "master"."dbo"."SSN"	1

Records 1 to 1 of 1



SSNID	LastNa	FirstNa	SSN_Num
0	Anthony	joe	123-45-6780
1	Thomas	joe	123-45-6781
2	Smith	Joe	123-45-6782
3	Jones	Joe	123-45-6783
4	Craven	Joe	123-45-6784
5	Shapiro	Joe	123-45-6785
6	King	Joe	123-45-6786
7	Lynch	Joe	123-45-6787
8	Williams	Joe	123-45-6788
9	Davis	Joe	123-45-6789
10	Wilson	Joe	234-56-7810



End Users	Access to excessive or unneeded data
	Data access outside standard hours
	Access via inappropriate or nonapproved channels

Guardium
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

Developers Sys. Admins Analysts	Access to live production systems

Developers/SAs/Analysts - Access to Live Production Systems

Start Date: **2010-03-07 20:53:45** End Date: **2010-03-12 17:53:45**

Timestamp	Client IP	Server IP	Network Protocol	Uid Chain Compressed	OS User	DB User Name	Source Program	Full Sql	Uid Chain
2010-03-11 20:47:40.0	10.10.9.56	10.10.9.56	BEQUEATH	joe	ORACLE	SYSTEM	SQLPLUS@OSPREY	select * from creditcard	(1,root,init [3])->(2267,root,/usr/sbin/sshd)->(20063,root,sshd: joe [priv])->(20065, joe,sshd: joe@pts/3)->(20066,joe,-bash)->(20142,joe,su - oracle)->(20149,oracle,-bash)->(20175, oracle,sqlplus)->(20182,oracle,oracleXE (DESCRIPTION=(LOCAL=YES)(ADDRESS= (PROTOCOL=beq))))

```
joe@osprey:~
Using username "joe".
joe@10.10.9.56's password:
Last login: Fri Sep 25 13:31:39 2009 from jdi
[joe@osprey ~]$ su - oracle
Password:
-bash-3.00$ sqlplus system

SQL*Plus: Release 10.2.0.1.0 - Production on Fri Mar 12 16:35:5

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

Enter password:

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

SQL> select * from creditcard;

NAME                                               CARDNUMBER          CARDID
-------------------------------------------------- ------------------ ----------
Joe D                                              1234567890123456            1
Harry S                                            2345678901234567            2

SQL> quit
Disconnected from Oracle Database 10g Express Edition Release 10.2.0.1.0 - Production
```

Developers Sys. Admins Analysts — Access to live production systems

What's wrong with the access to this production server?

- DB User = System account with access to production
- Table accessed Creditcard = All creditcard accounts
- Source Program = SQLPLUS, not the creditcard app
- Generic Accounts – Who did it? (Joe)

Guardium® SAFEGUARDING DATABASES™ | AN IBM® COMPANY

IT Ops	Nonapproved changes to databases or applications
	Out-of-cycle patching of production systems

IT Operations- Unapproved Changes to DB and Apps Files (File Integrity Monitoring)

CAS Change Details

Start Date: **2008-10-15 00:00:00** End Date: **2008-10-15 11:49:27**

Host_Name	Monitored_Item	OS_Type	DB_Type	Instance_Name	Type	Owner	Last_Modified_Time	Sample_Time	Permissions
10.10.9.56	/usr/lib/oracle/xe/app/oracle/product/10.2.0/server/network/admin/listener.ora	UNX	N/A	listener.ora instance	File	nicholas	2008-10-15 11:31:28.0	2008-10-15 11:43:29.0	-rwxr-xr-x

```
root@osprey:/usr/lib/oracle/xe/app/oracle/product/10.2.0/server/network/admin
[root@osprey admin]# chmod 777 listener.ora
[root@osprey admin]# ls -l listener.ora
-rwxrwxrwx  1 nicholas dba 578 Oct 15 11:31 listener.ora
[root@osprey admin]#
```

CAS Change Details

Start Date: **2008-10-15 00:00:00** End Date: **2008-10-15 12:14:55**

Host_Name	Monitored_Item	OS_Type	DB_Type	Instance_Name	Type	Owner	Last_Modified_Time	Sample_Time	Permissions
10.10.9.56	/usr/lib/oracle/xe/app/oracle/product/10.2.0/server/network/admin/listener.ora	UNX	N/A	listener.ora instance	File	nicholas	2008-10-15 11:31:28.0	2008-10-15 11:53:53.0	-rwxrwxrwx
10.10.9.56	/usr/lib/oracle/xe/app/oracle/product/10.2.0/server/network/admin/listener.ora	UNX	N/A	listener.ora instance	File	nicholas	2008-10-15 12:02:52.0	2008-10-15 12:03:49.0	-rwxrwxrwx

Records: 5 to 6 of 6

IT Ops	Nonapproved changes to databases or applications
	Out-of-cycle patching of production systems

Guardium SAFEGUARDING DATABASES™ AN IBM® COMPANY

IT Operations- Unapproved Changes to Database Files

Saved_Data_Id	Host_Name	Monitored_Item	Saved_Data	Last_Modified_Time	Sample_Time	Owner	Permissions	Timestamp	Size	Group	of Saved Datas
147	10.10.9.56	/usr/lib/oracle/xe/app/oracle/product/10.2.0/server/network/admin/listener.or	# listener.ora Network Configuration File: SID_LIST_LISTENER = (SID_LIST = (SID_DESC = (SID_NAME = PLSExtProc) (ORACLE_HOME = /usr/lib/oracle/xe/app/oracle/product/10.2.0/serve (PROGRAM = extproc))) LISTENER = (DESCRIPTION_LIST = (DESCRIPTION = (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC_FOR_XE)) (ADDRESS = (PROTOCOL = TCP)(HOST = osprey) (PORT = 1521)))) LISTENER = (DESCRIPTION_LIST = (DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = osprey) (PORT = 1529)))) DEFAULT_SERVICE_LISTENER = (XE)	2008-10-15 12:02:52.0	2008-10-15 12:03:49.0	nicholas	-rwxrwxrwx	2008-10-15 12:04:39.0	578	dba	1
146	10.10.9.56	/usr/lib/oracle/xe/app/oracle/product/10.2.0/server/network/admin/listener.ora	# listener.ora Network Configuration File: SID_LIST_LISTENER = (SID_LIST = (SID_DESC = (SID_NAME = PLSExtProc))) LISTENER = (DESCRIPTION_LIST = (DESCRIPTION = (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC_FOR_XE)) (ADDRESS = (PROTOCOL = TCP)(HOST = osprey) (PORT = 1521)))) LISTENER = (DESCRIPTION_LIST = (DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = osprey) (PORT = 1525))))	2008-10-15 11:31:28.0	2008-10-15 11:53:53.0	nicholas	-rwxrwxrwx	2008-10-15 11:54:45.0	578	dba	1

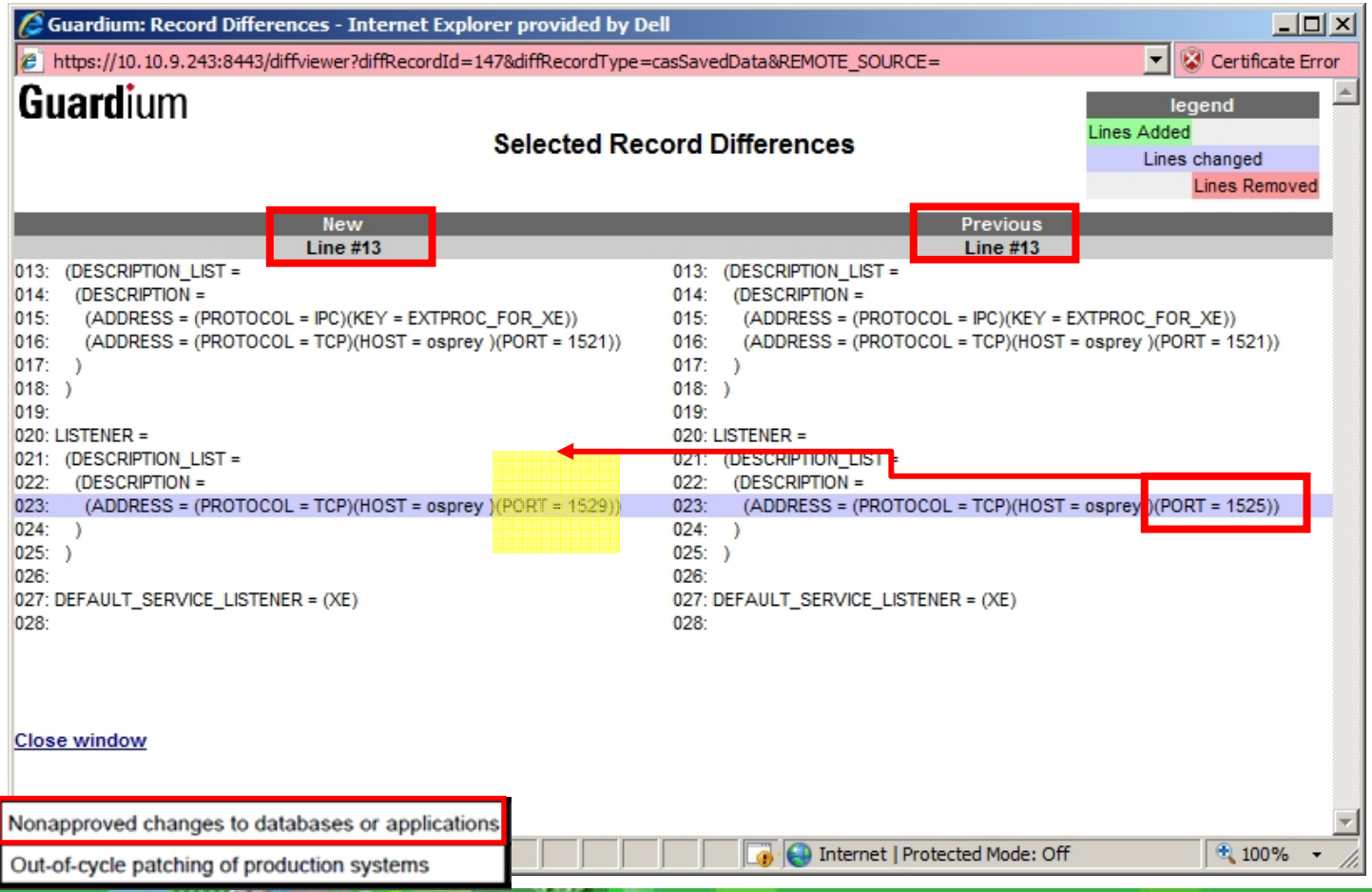
Contents of the Listener.ora file

View Difference

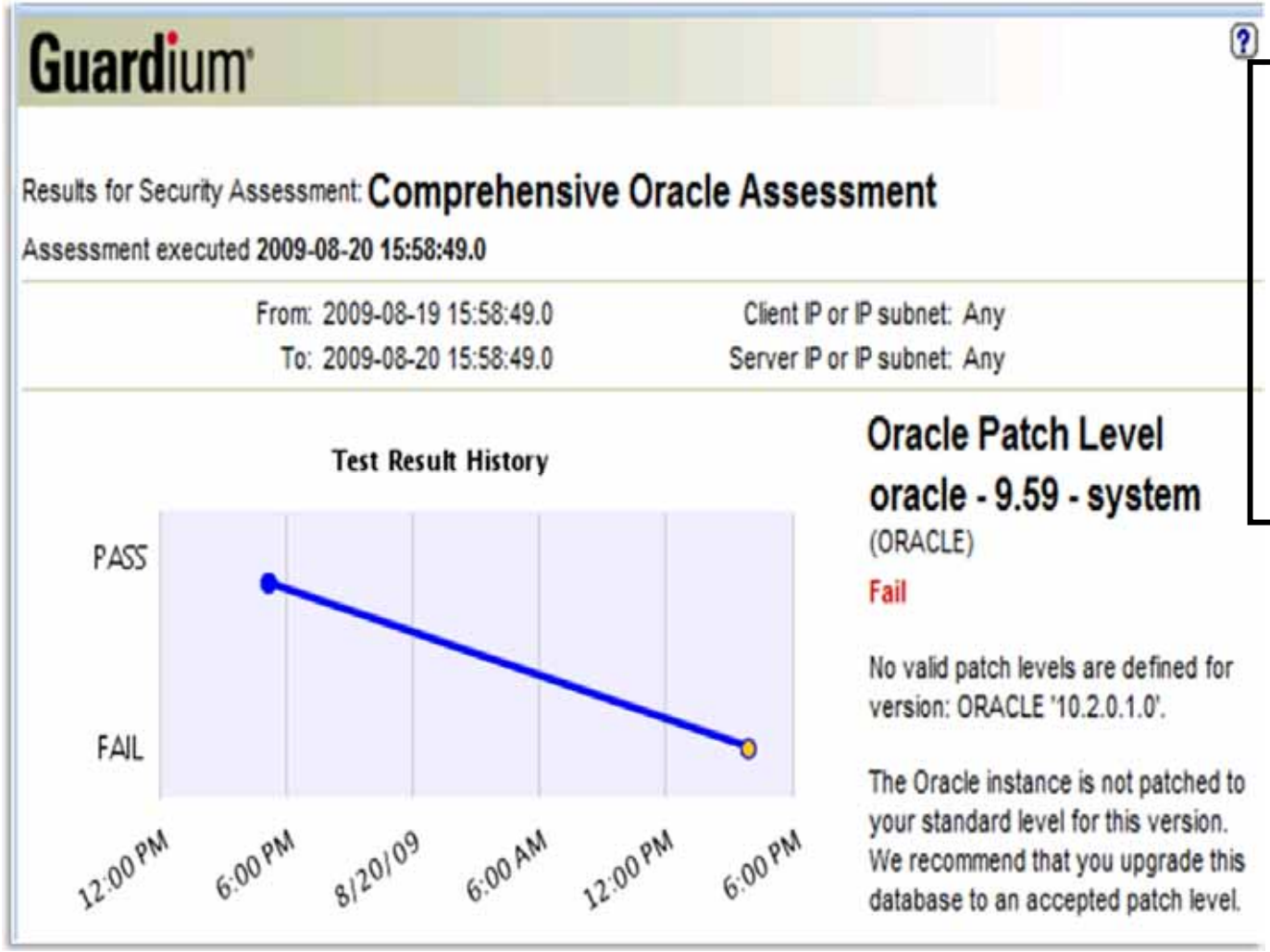
IT Ops	Nonapproved changes to databases or applications
	Out-of-cycle patching of production systems

Difference Report Shows Changes in the Listener.ora File

- (ADDRESS = (PROTOCOL = TCP)(HOST = osprey)(PORT = 1525))
- (ADDRESS = (PROTOCOL = TCP)(HOST = osprey)(PORT = 1529))



Patch History Changed – From Pass to Fail!



- Patch was applied to production server, but not fully tested and approved according to corporate policy

IT Ops	Nonapproved changes to databases or applications
	Out-of-cycle patching of production systems

The Enterprise Patching Issue

- Nearly half of companies lack a formal patch management process
- 62% typically take 3 months or more to apply Critical Patch Updates (IOUG)
- Only 18% measure patch success via configuration scanning
- "The least mature areas of patching seem to correlate almost directly with the fastest-growing areas of attacks, such as … database servers [and] business application servers."

"Patch management is one of the most fundamental functions of IT departments, yet in our research we discovered it remains one of the biggest pain points for many organizations."

Rich Mogull, Securosis

http://www.darkreading.com/database_security
http://www.securosis.com/projectquant
http://ioug.itconvergence.com/pls/apex/ESIG.download_my_file?p_file

Don’t Forget the Database Danger from Within

- “Organizations overlook the most imminent threat to their databases: authorized users.” (Dark Reading)
- 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)
- “No one group seems to own database security…This is not a recipe for strong database security”…63% depend primarily on manual processes.” (ESG)

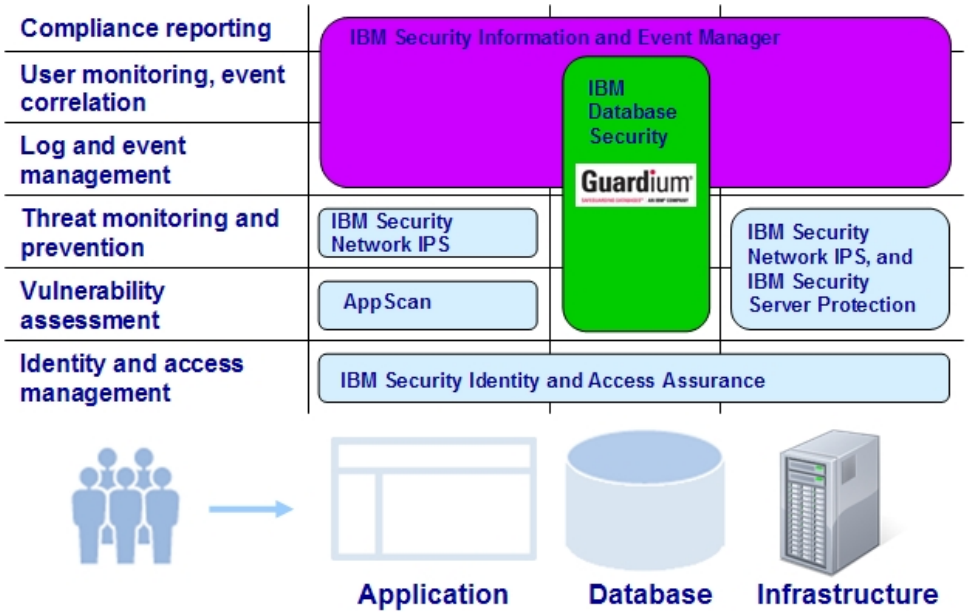
http://www.guardium.com/index.php/landing/866/

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

DAM Provides a Simple Means of Centralizing and Automating Controls

- Discovering and applying controls to all sensitive data
- Controlling who accesses and modifies what data, from where, and when
- Managing exposure to misuse of credentials, privileges, etc.
- Ensuring sensitive data stores are appropriately configured
- Standardizing, automating and streamlining the review and remediation of policy violations, as well compliance validation activities
- Without compromising separation of duties or performance

IBM Integrated Solution – Enterprise User Activity Monitoring



- Enterprise dashboard with compliance management modules and regulation-specific reports
- Broadest coverage, collecting and correlating native logs and events across systems, devices, middleware and applications
- With Guardium, IBM:
  - Monitors all DB activities in *real-time*, including privileged users, without the performance impact and separation of duties issues of native DB logging
  - Provides capabilities such as blocking, workflow management and vulnerability assessments

Integrated Solution Facts:

- IBM Tivoli Security Information and Event Manager Enterprise dashboard and compliance reports fully support Guardium events
- Integration is available now

Guardium collected data in SIEMv2

generated by iView v2.0 on TSIEMVM at Thursday, March 25, 2010 11:58:28 PM CDT
database CIFDB:Windows
loading date: 3/25/10 11:53:16 PM (-0500)
data range: 12/7/09 11:00:00 AM (-0500) - 12/7/09 11:00:00 AM (-0500)
CIFDB Windows All Events

All Events

Database Windows on Server CIFDB

Setup:

	Month	Day	Year	Hour	Min
Start time	December	7	2009	10	0
End time	December	7	2009	10	0

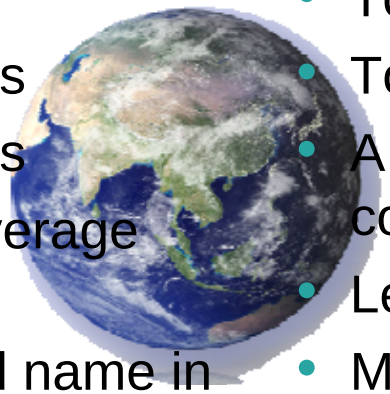
Time zone: Event time zone

Severity	Date / Time	#	What (detail)	Where (detail)	Who (detail)	Where From (detail)	On What (detail)	Where To (detail)
10	12/7/09 11:00:00 AM (-0500)	1	Login : User / Failure	ORACLE (ORACLE)	John Smith	10.10.9.56	Database : - / ORACLE	10.10.9.244 (ORACLE)
10	12/7/09 11:00:00 AM (-0500)	1	Login : User / Failure	ORACLE (ORACLE)	APPS	192.168.30.61	Database : - / ORACLE	192.168.2.148 (ORACLE)
10	12/7/09 11:00:00 AM (-0500)	1	Login : User / Failure	ORACLE (ORACLE)	appuser	10.10.9.56	Database : - / ORACLE	10.10.9.56 (ORACLE)
10	12/7/09 11:00:00 AM (-0500)	1	Login : User / Failure	MYSQL (MYSQL)	bob	10.10.9.56	Database : - / MYSQL	10.10.9.56 (MYSQL)

Guardium, an IBM Company

The database protection and compliance solution chosen by leading organizations world-wide:

- 4 of the top 5 global banks
- 2 of the top 3 global retailers
- 4 of the top 6 global insurers
- 2 of the world's favorite beverage brands
- One of the most recognized name in PCs
- 25 of the world's leading telcos



- Top government agencies
- Top 3 auto maker
- A top dedicated security company
- Leading energy suppliers
- Major health care providers
- Media & entertainment brands

More Information Available

- www.guardium.com
  - Free on demand webcasts: SOX, PCI DSS compliance, …
  - Free analyst reports: creating a database security plan (Forrester), database risk study (ESG), ….
  - ROI and application case studies
- Sign-up for a free hands-on POT learning lab (a full day of hands on with the technology)
    - Sydney - Monday 16th August
    - Melbourne - Friday 20th August
    - elsewhere let me know
  - Contact Scott Henley (scott.henley@au1.ibm.com)

The Case for Database Activity Monitoring

Scott Henley
scott.henley@au1.ibm.com