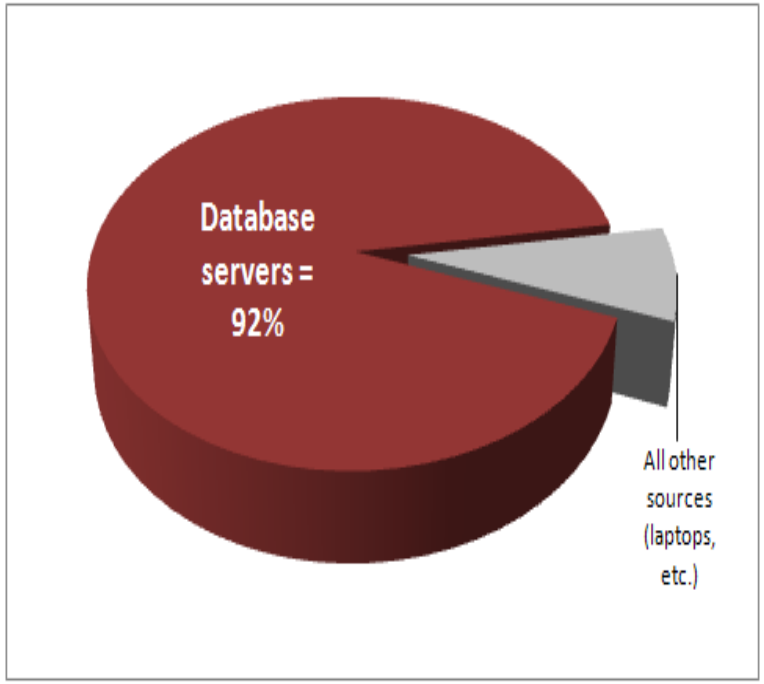
Database Protection

Scott Henley CISSP, CISA
IBM Security Architect
19/5/2011

The IBM SecurityStudio Tackling the illusion of absolute security

Database Servers Are The Primary Source of Breached Data

Source of Breached Records



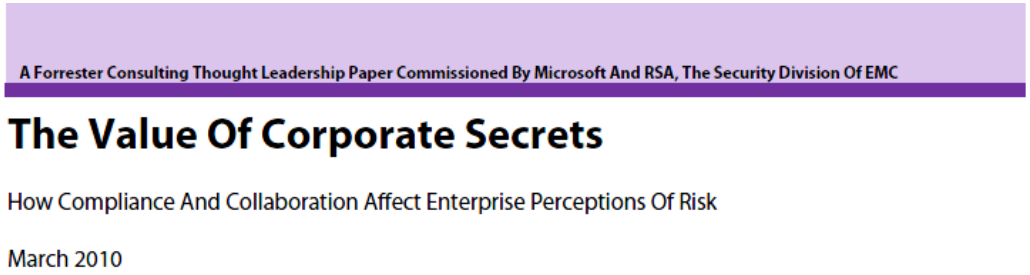
2010 Data Breach Report from Verizon Business RISK Team

http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

… up from 75% in 2009 Report

"Although much angst and security funding is given to **mobile devices and end-user systems,** these assets **are simply not a major point of compromise."**

Cost of a Data Breach


A Forrester Consulting Thought Leadership Paper Commissioned By Microsoft And RSA, The Security Division Of EMC

The Value Of Corporate Secrets

How Compliance And Collaboration Affect Enterprise Perceptions Of Risk

March 2010

Forrester survey of 305
IT decision makers*:

- Companies focus mainly on preventing accidents (email, etc.) but deliberate/unknowing theft of information by trusted employees more costly
  - Damage caused by rogue IT administrator = $482K (average)
  - Average cost of accidental leakage = $12K
- Secrets (e.g. strategic plans) are twice as valuable as custodial data (personal information, credit card data, etc.)
- Most CISOs don't really know if their controls really work

* Note: Survey does not address other costs such as fines

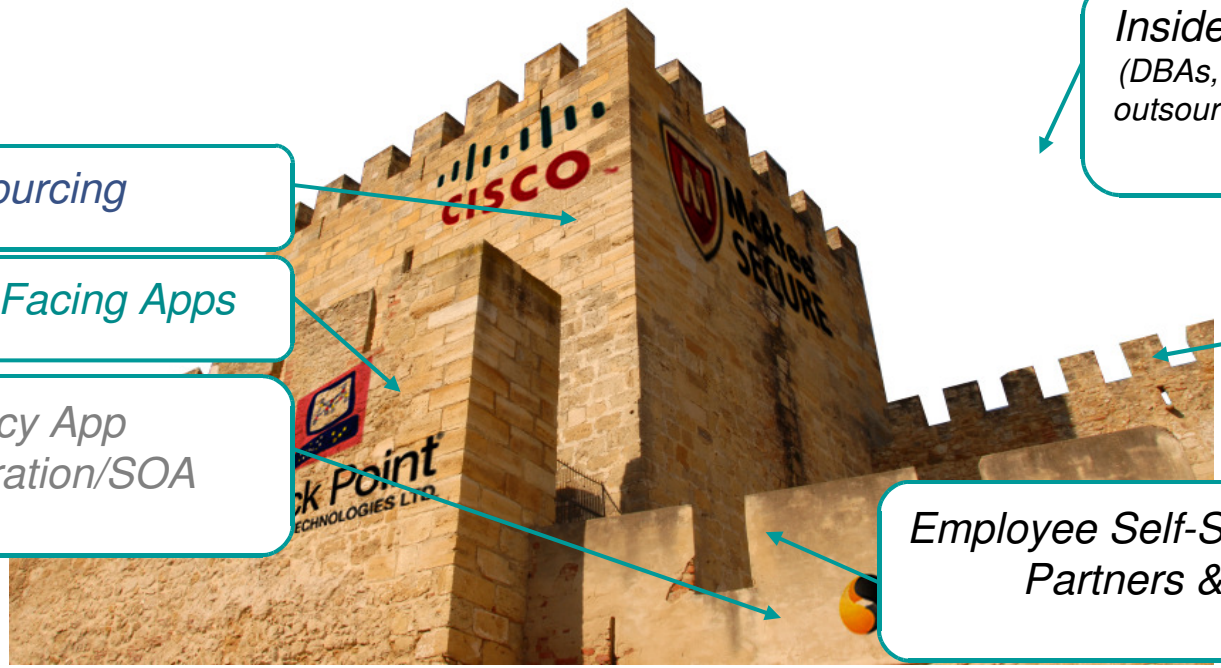
Ponemon CODB 2010 study:

- average cost of a data breach in the US has gone up to 7.2M (up 7% from 6.8M in 2009)
- on average $214 per compromised record (up about $10 per record from 2009)

Perimeter Defences No Longer Sufficient

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

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



Insiders
(DBAs, developers, outsourcers, etc.)

Outsourcing

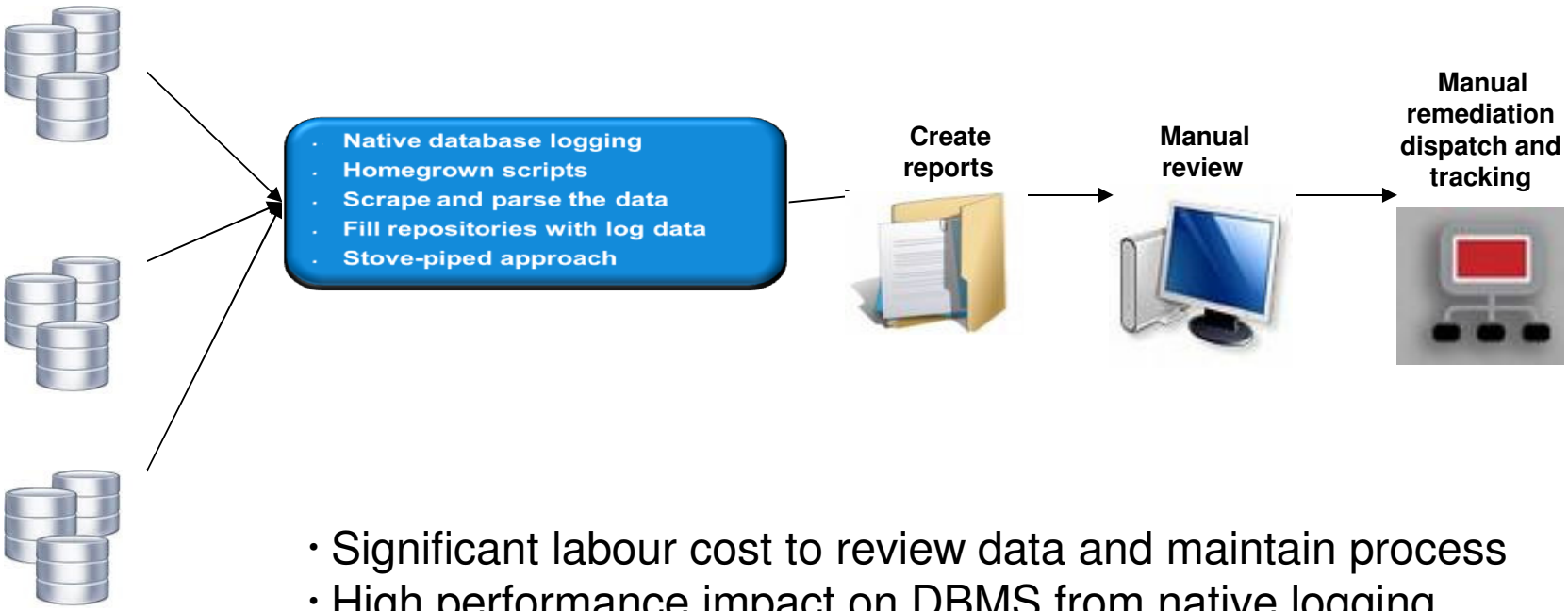
Web-Facing Apps

Legacy App Integration/SOA

Stolen Credentials
(Zeus, etc.)

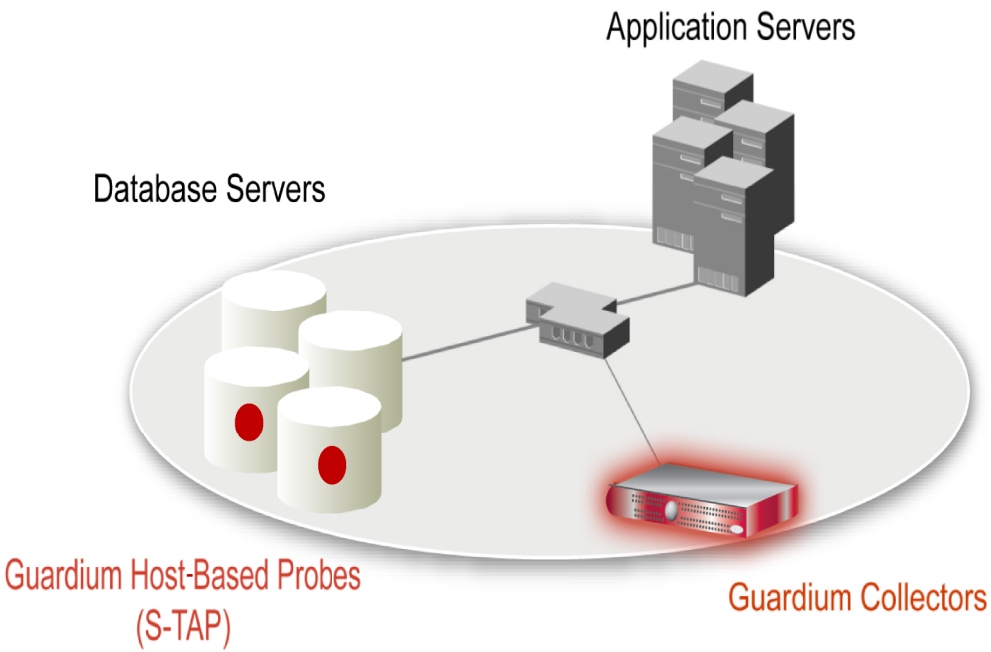
Employee Self-Service, Partners & Suppliers

Current Solutions Are Costly and Ineffective



- Significant labour cost to review data and maintain process
- High performance impact on DBMS from native logging
- Not real-time
- Does not meet auditor requirements for Separation of Duties
- Audit trail is not secure
- Inconsistent policies enterprise-wide

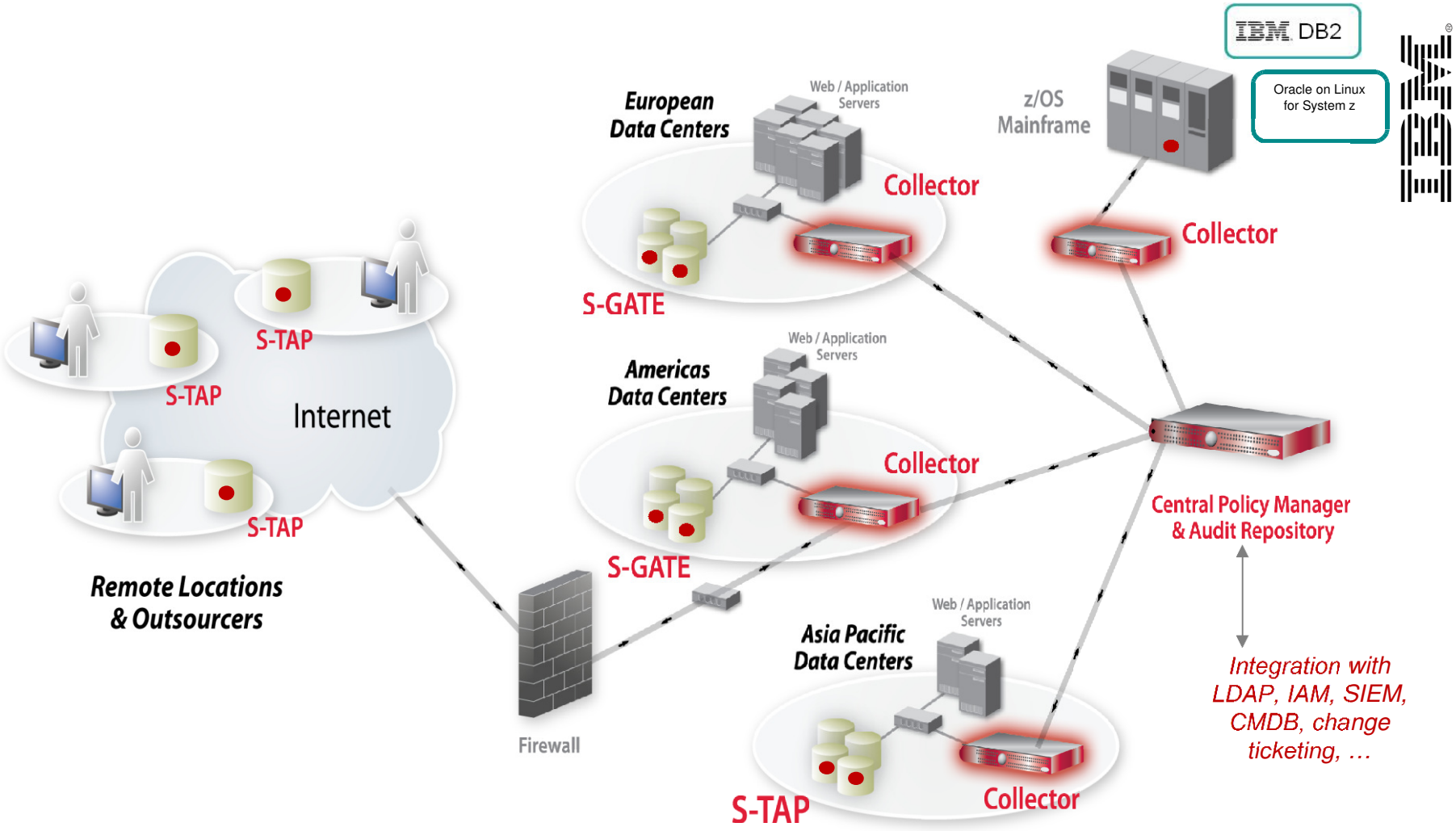
IBM InfoSphere Guardium:
Non-Invasive, Real-Time Database Security & Monitoring



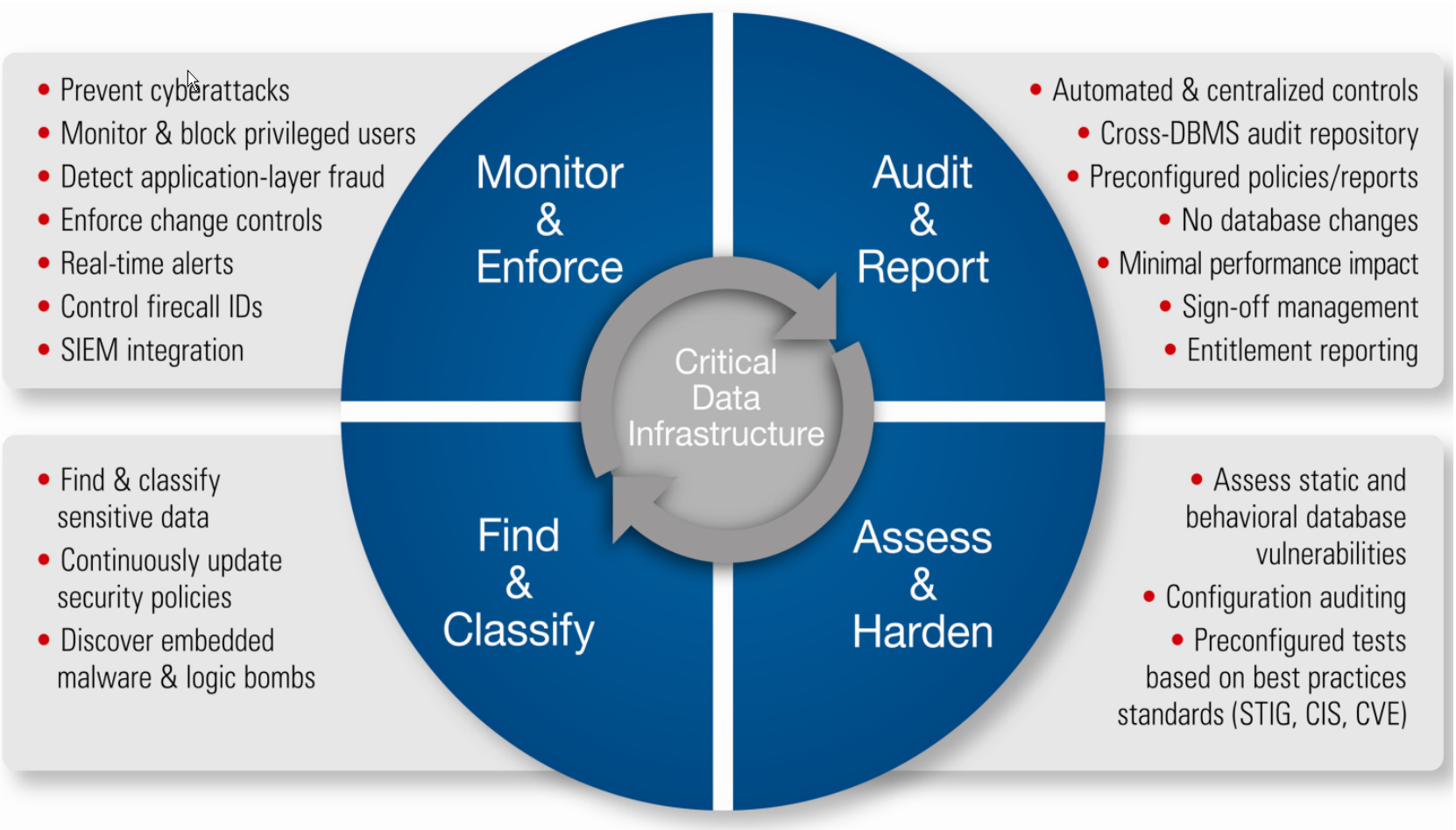
- Continuously monitors <u>all</u> database activities (including local access by superusers)
- Heterogeneous, cross-DBMS solution
- Does not rely on native DBMS logs
- Minimal performance impact (2-3%)
- No DBMS or application changes

- Activity logs can't be erased by attackers or DBAs
- Automated compliance reporting, sign-offs & escalations (SOX, PCI, NIST, etc.)
- Granular, real-time policies & auditing
  - *Who, what, when, where, how*

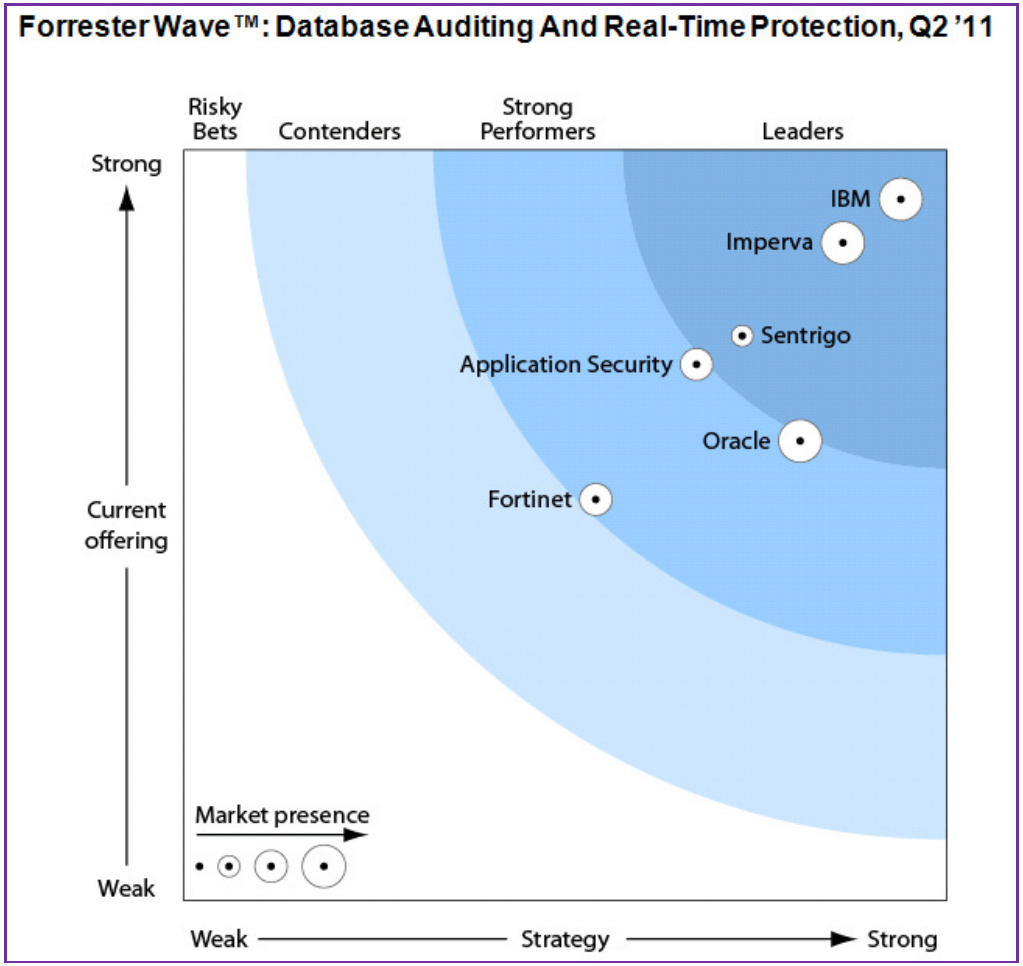
Scalable Multi-Tier Architecture



Guardium Addresses the DB Security Lifecycle



InfoSphere Guardium Continues to Demonstrate It's Leadership…



2007

Source: The Forrester Wave™: Database Auditing And Real-Time Protection, Q2 2011, May 6, 2011. The Forrester Wave is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on best available resources. Opinions reflect judgement at the time and are subject to change.

Achieving the Highest Rankings in 15 of 17 High Level Categories Evaluated

- Awarded highest score in overall “Market Presence”
- Awarded highest score in overall “Strategy”
- Awarded highest score in evaluation of “Current Offering”
- Achieved highest score possible in 8 out of 16
- Achieved the top ranking in 7
- Evaluation based on v7, v8 introduced weeks after cutoff

The Forrester Wave™: Database Auditing And Real-Time Protection, Q2 2011, May 6, 2011. Forrester Research, Inc.

The Evaluation Process

- 6 of the top vendors evaluated
- Examined past research
- Customer reference calls
- Conducted user needs assessments
- Conducted vendor and expert interviews
- Examined product demos
- Conducted lab evaluations
- 147 evaluation criteria

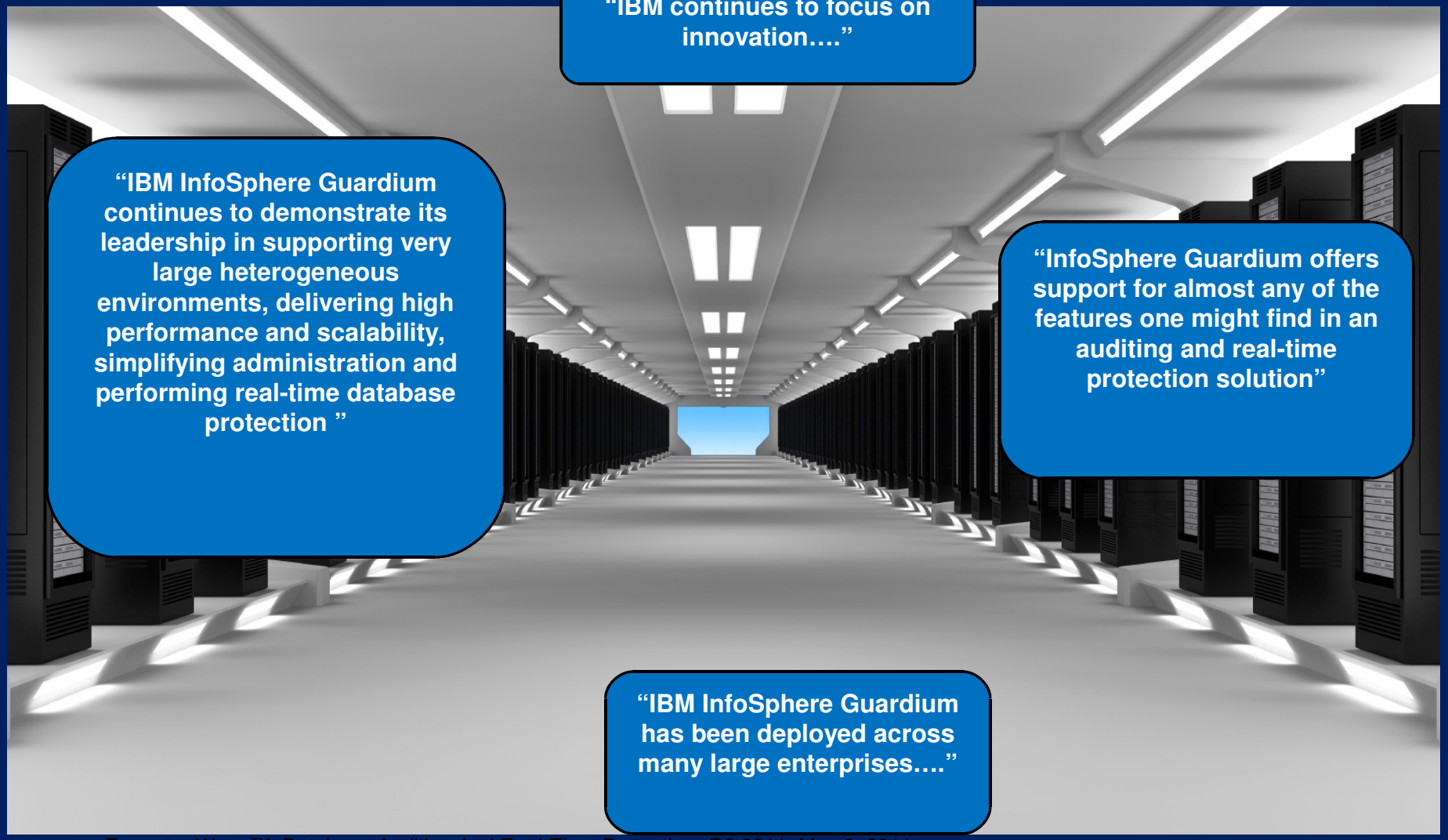
Vendors Evaluated Against 147 Criteria in 3 Categories

	Forrester's Weighting	IBM
CURRENT OFFERING	50%	4.67
Database auditing	10%	4.88
User and application auditing	15%	4.68
Audit policies	10%	5.00
Auditing repository	10%	5.00
Reporting and analytics	10%	4.76
Real-time protection	15%	4.80
Architecture	15%	4.19
Manageability	15%	4.40
STRATEGY	50%	4.70
Product strategy	60%	4.50
Corporate strategy	40%	5.00
Cost	0%	0.00
MARKET PRESENCE	0%	4.92
Installed base	20%	5.00
Revenue	10%	4.20
Services	20%	5.00
Employees	20%	5.00
Technology partners	20%	5.00
International presence	10%	5.00

All scores are based on a scale of 0 (weak) to 5 (strong).

The Forrester Wave™: Database Auditing And Real-Time Protection, Q2 2011, May 6, 2011. Forrester Research, Inc.

“IBM’s Acquisition of Guardium in 2009 Changed Everything, Making IBM one of the Leading Players”



“IBM continues to focus on innovation….”

“IBM InfoSphere Guardium continues to demonstrate its leadership in supporting very large heterogeneous environments, delivering high performance and scalability, simplifying administration and performing real-time database protection ”

“InfoSphere Guardium offers support for almost any of the features one might find in an auditing and real-time protection solution”

“IBM InfoSphere Guardium has been deployed across many large enterprises….”

Forrester Wave™: Database Auditing And Real-Time Protection, Q2 2011, May 6, 2011.

Example use cases....

Guardium Assessment Results

Guardium

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

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

-- Select another result --

From: 2009-08-20 12:47:28.0
To: 2009-08-21 12:47:28.0

Client IP or IP subnet: Any
Server IP or IP subnet: Any

Download PDF

Historical Progress or Regression

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

Tests passing: 100%, 80%, 60%, 40%, 20%, 0%

8/19/09, 8/20/09, 8/21/09, 8/22/09

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

Filter control for easy use

Show only: Reset Filtering

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

Sort by:

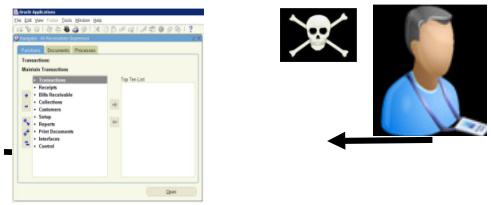
First	Second	Third
Severity	Score	Datasource

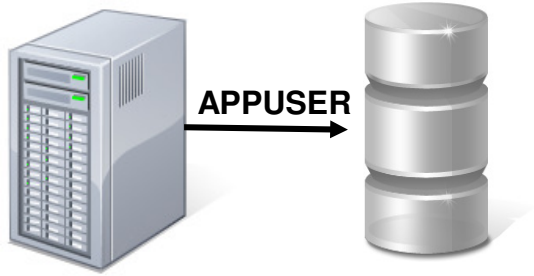
Apply

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

Cat.	Test Name	Datasource	P/F	Sev.	Reason
Other	Excessive Login Failures (Production)	[Observed]	Fail	Critical	Too Many login failures, found 15 per day. *Recommendation: An alarming number of login failures have been reported from your databases. This might be an indication of an attempt to break into your database, or of someone trying to steal or damage your data. The number of login failures should be close to zero, especially in production environments. You should immediately inspect all attempts to access your database and the source of all the login failures, and take immediate action to deny access to your database from unauthorized clients.*
Conf.	DBA Profile FAILED_LOGIN_ATTEMPTS Are Limited	ORACLE: oracle - 9.59	Fail	Critical	User profile [MONITORING_PROFILE] setup parameter FAILED_LOGIN_ATTEMPTS found out of defined threshold value

Granular Policies with Detective & Preventive Controls





Application Server 10.10.9.244

Database Server 10.10.9.56

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

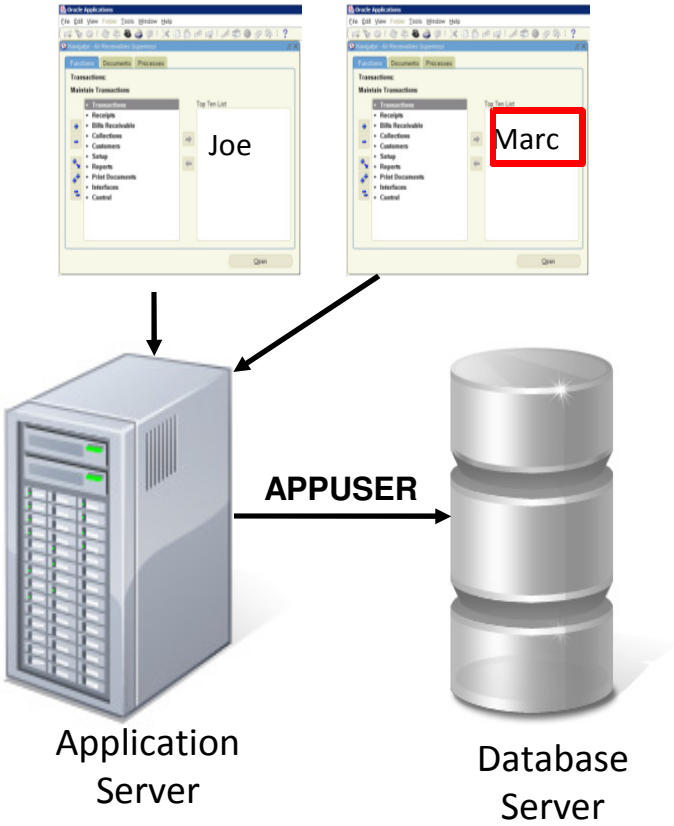
ALERT DAILY
ALERT ONCE PER SESSION
ALERT PER MATCH
ALERT PER TIME GRANULARITY
ALLOW
IGNORE RESPONSES PER SESSION
IGNORE SESSION
IGNORE SQL PER SESSION
LOG FULL DETAILS
LOG FULL DETAILS PER SESSION
LOG FULL DETAILS WITH VALUES
LOG FULL DETAILS WITH VALUES PER SESSION
LOG MASKED DETAILS
LOG ONLY
RESET
S-GATE ATTACH
S-GATE DETACH
S-GATE TERMINATE
S-TAP TERMINATE
SKIP LOGGING

Sample Alert

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

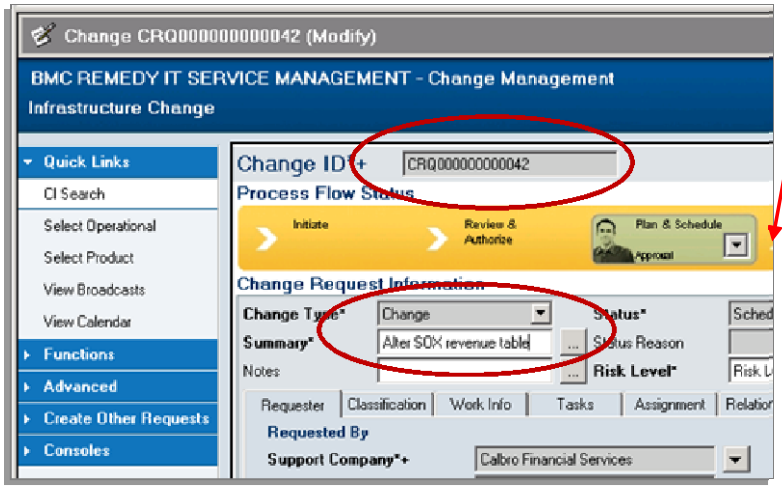
Identifying Fraud at the Application Layer



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 …)
  - No changes required to applications
  - Deterministic tracking of user IDs
    - Does not rely on time-based "best-guess"

Enforcing Change Control Policies



Tag DBA actions with ticket IDs

Compare observed changes to approved changes

Identify unauthorized changes (red) or changes with invalid ticket IDs

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 15:41:55.0	ORACLE	0	0			crq000000000232	allen	SYSTEM	192.168.8.129	192.168.8.129	Alter table sox_sales_international add total_rev float
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(?,?,?,?,?,?

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?

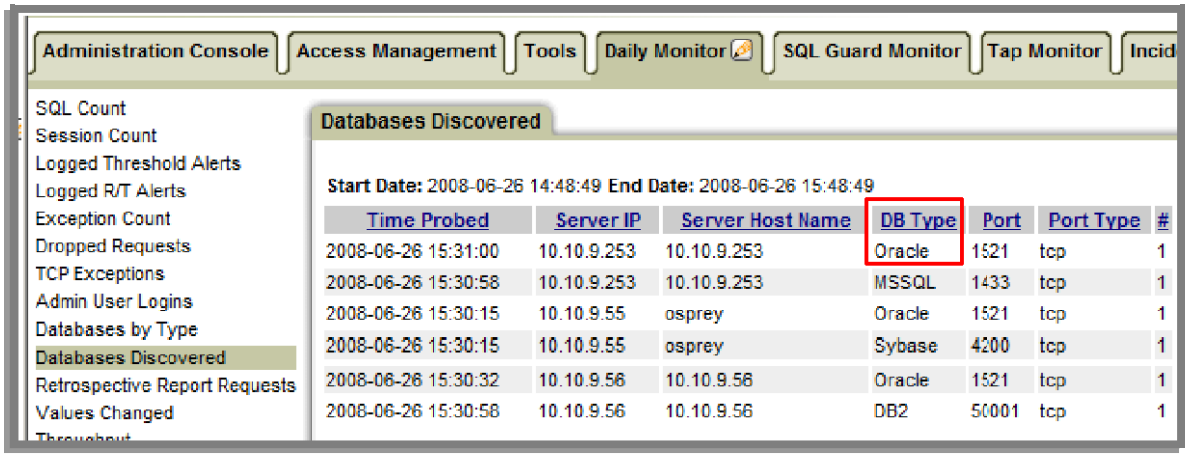
HARRY	select * from ar.creditcard where i<?	**********0002, **********0003, **********0004
JOE	select * from ar.creditcard where i<?	**********0001
JOE	select * from ar.creditcard where i<?	**********0002, **********0003, **********0004, **********0005, **********0006, **********0007, **********0008, **********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

Auditing Database Configuration Changes

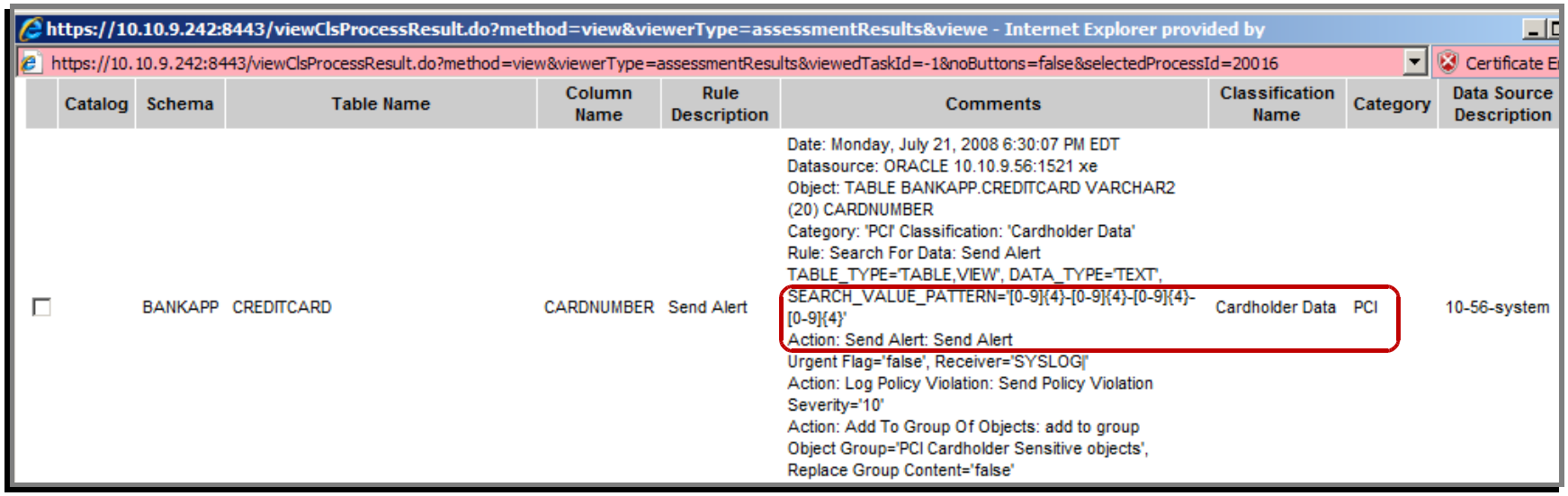
$ORACLE_HOME/soap/bin/.*	File Pattern	12h	✓	✓
$ORACLE_HOME/sysman/admin/OMSRepositoryConstraints.properties	File Pattern	12h	✓	✓
$ORACLE_HOME/sysman/config/.*properties	File Pattern	12h	✓	✓
$ORACLE_HOME/xdk/admin/xml.properties	File Pattern	12h	✓	✓
ORACLE_BASE	Environment Variable	12h	✓	⊘
ORACLE_HOME	Environment Variable	12h	✓	⊘
ORACLE_SID	Environment Variable	12h	✓	⊘
TNS_ADMIN	Environment Variable	12h	✓	⊘
select * from dba_db_links	SQL Script	12h	✓	⊘

- Track changes to files, environment variables, registry settings, scripts, etc. that can affect security posture
- 200+ pre-configured, customizable templates for all major OS/DBMS configurations

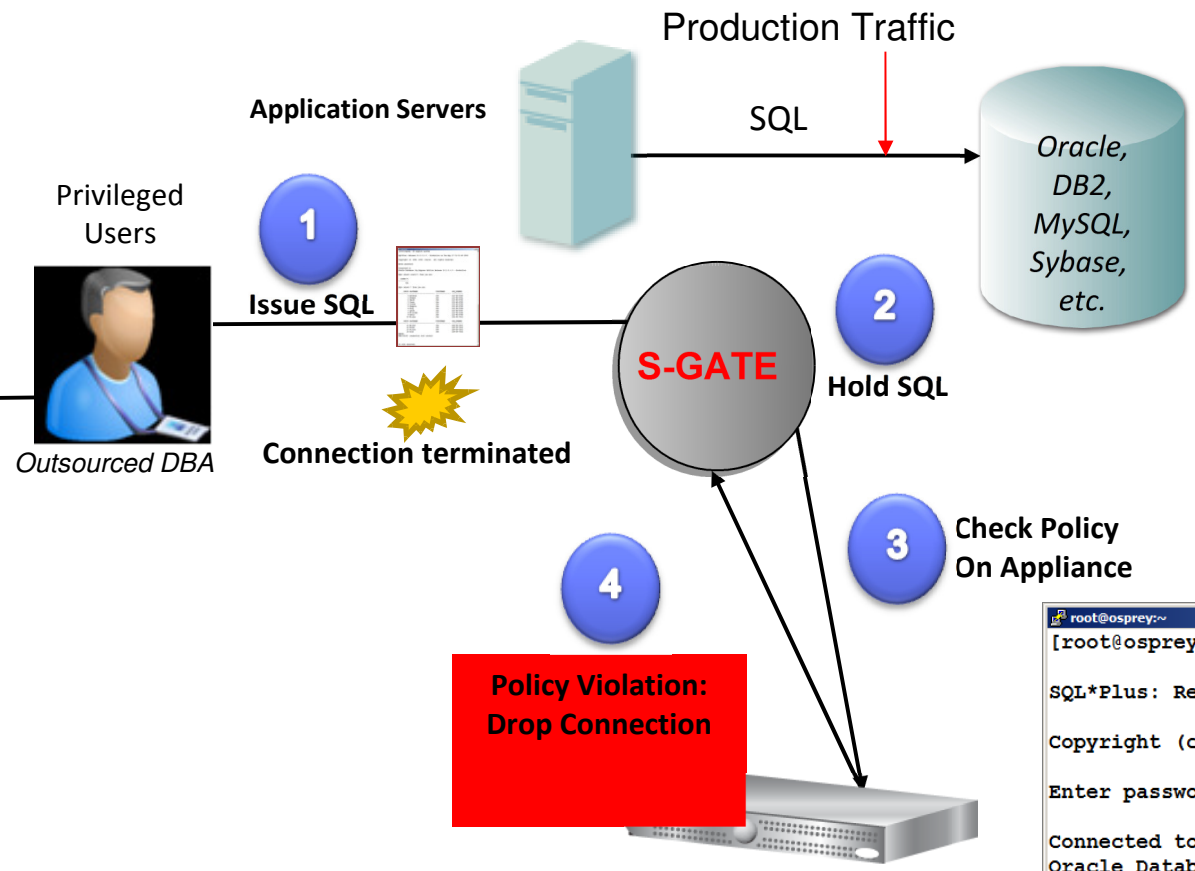
Discovering & Classifying Sensitive Data



- ✓ Discover databases
- ✓ Discover sensitive data
- ✓ Policy-based actions
  - ✓ Alerts
  - ✓ Add to group of sensitive objects



Proactively Preventing Policy Violations in Real-time



- ✓ No database changes
- ✓ No application changes
- ✓ Without risk of inline appliances that can interfere with application traffic

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

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

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

Enter password:

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

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

SQL>
```

Session Terminated

Common Attack Patterns

- **Thwart intruders that impersonate Application Servers,** hijack Views and Triggers, or *su* (Switch User) to generic IDs in order to conceal their actions

Identifying Users That “su”

```
joe@osprey:~
login as: joe
joe@10.10.9.56's password:
Last login: Tue Sep 22 01:07:26 2009 from jdi
[joe@osprey ~]$ su - oracle
Password:
-bash-3.00$ sqlplus system

SQL*Plus: Release 10.2.0.1.0 - Production on Tue Sep 22 01:12:24 2009

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> create view PatientView as select * from joe.patient;

View created.

SQL> select firstname,lastname,cardnumber,ssn from PatientView where Patientid=3;

FIRSTNAME       LASTNAME                  CARDNUMBER                SSN
--------------- ------------------------- ------------------------- -----------
Joe             Jones                     4486742167789074          456-78-9012
```

- SQL Trace SQL

Start Date: **2009-09-16 01:20:49** End Date: **2009-09-22 02:20:49**

Timestamp	Client IP	Server IP	Network Protocol	Service Name	Source Program	Uid Chain	Uid Chain Compressed	OS User	DB User Name	Full Sql
2009-09-22 01:12:55.0	10.10.9.56	10.10.9.56	BEQUEATH	ORACLEXE	SQLPLUS@OSPREY	(1,root,init [3])->(2323,root,/usr/sbin/sshd)->(26770,root,sshd: joe [priv])->(26778, joe,sshd: joe@pts/2)->(26779,joe,-bash)->(26817,joe,su - oracle)->(26818,oracle,-bash)->(26844, oracle,sqlplus)->(26851,oracle,oracleXE (DESCRIPTION=(LOCAL=YES)(ADDRESS=(PROTOCOL=beq))))	joe	ORACLE	SYSTEM	create view PatientView as select * from joe.patient

Attacker Creates a View (Indirect Access)

joe@osprey:~

```
login as: joe
joe@10.10.9.56's password:
Last login: Tue Sep 22 01:07:26 2009 from jdi
[joe@osprey ~]$ su - oracle
Password:
-bash-3.00$ sqlplus system
```

Policy Violations Details

Start Date: **2009-08-27 00:00:00** End Date: **2009-09-22 01:59:40**

Timestamp	Category Name	Access Rule Description	Client IP	Server IP	DB User Name	Full SQL String	Severity Description
2009-09-22 01:12:55.0		Alert on Creation of Tables from Unauthorized Source	10.10.9.56	10.10.9.56	SYSTEM	create view PatientView as select * from joe.patient	HIGH

```
Oracle Database 10g Express Edition Release 10.2.0.1.0 - Production

SQL> create view PatientView as select * from joe.patient;

View created.

SQL> select firstname,lastname,cardnumber,ssn from PatientView where Patientid=3;

FIRSTNAME       LASTNAME                  CARDNUMBER                SSN
--------------- ------------------------- ------------------------- -----------
Joe             Jones                     4486742167789074          456-78-9012
```

- SQL Trace SQL

Start Date: **2009-09-16 01:20:49** End Date: **2009-09-22 02:20:49**

Timestamp	Client IP	Server IP	Network Protocol	Service Name	Source Program	Uid Chain	Uid Chain Compressed	OS User	DB User Name	Full Sql
2009-09-22 01:14:42.0	10.10.9.56	10.10.9.56	BEQUEATH	ORACLEXE	SQLPLUS@OSPREY	(1,root,init [3])->(2323,root,/usr/sbin/sshd)->(26770,root,sshd: joe [priv])->(26778, joe,sshd: joe@pts/2)->(26779,joe,-bash)->(26817,joe,su - oracle)->(26818,oracle,-bash)->(26844, oracle,sqlplus)->(26851,oracle,oracleXE (DESCRIPTION=(LOCAL=YES)(ADDRESS=(PROTOCOL=beq))))	joe		ORACLE SYSTEM	select firstname,lastname,cardnumber,ssn from PatientView where Patientid=3

Capturing Data Leakage

joe@osprey:~

```
login as: joe
joe@10.10.9.56's password:
Last login: Tue Sep 22 01:07:26 2009 from jdi
[joe@osprey ~]$ su - oracle
Password:
-bash-3.00$ sqlplus system

SQL*Plus: Release 10.2.0.1.0 - Production on Tue Sep 22 01:12:24 2009

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> create view PatientView as select * from joe.patient;

View created.

SQL> select firstname,lastname,cardnumber,ssn from PatientView where Patientid=3;

FIRSTNAME       LASTNAME                  CARDNUMBER                SSN
--------------- ------------------------- ------------------------- -----------
Joe             Jones                     4486742167789074          456-78-9012

SQL>
```

Policy Violations Details

Start Date: **2009-08-27 00:00:00** End Date: **2009-09-22 01:59:40**

Timestamp	Category Name	Access Rule Description	Client IP	Server IP	DB User Name	Full SQL String	Severity Description
2009-09-22 01:14:42.0	data security	Alert on UnAuthorized Access to SSN	10.10.9.56	10.10.9.56	SYSTEM	select firstname,lastname,cardnumber,ssn from PatientView where Patientid=3 Extrusion Values: 456-78-****	HIGH

Automated Sign-offs & Escalations for Compliance

Guardium

Weekly Database Change Management Process
Audit process execution began 4/16/09 12:24 AM

Other Results For This Process

Sign Results | Continue | Escalate | Comment | Download PDF

Distribution Status:
Comments:

Timestamp	User	Comment for Result
2009-04-16 00:42:37.0	Marc	Need to review the DB login failure more closely! App User account should not fail a login.

Report: Database Changes Report [-ChangeRequest Report] Overall Value: 3
Security Assessment: Security Assessment [-Assessment] Overall Value: 36
Classification Process: Classification Process [Search for CreditCard Accounts - CreditCard Accounts]
Report: Failed DB Logins Report [Failed User Login Attempts] Overall Value: 1
Report: SQL Errors Report [SQL Errors] Overall Value: 56

Close this window

View

- Automates entire compliance workflow
  - Report distribution to oversight team
  - Electronic sign-offs
  - Escalations
  - Comments & exception handling

- Addresses auditors' requirements to document oversight processes
- Results of audit process stored with audit data in secure audit repository
- Streamlines and simplifies compliance processes

Optimizing Operations With TSIEM Integration

All Events - Database GEM on Server CIFDB - Microsoft Internet Explorer

File Edit View Favorites Tools Help

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

Dashboard Trends Reports Regulations Policy Groups Distribution Settings

CIFDB » GEM » All Events

All Events
Database GEM on Server CIFDB

Setup:

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

Execute Reset

Time zone: Event time zone

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

Local intranet

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

Introducing InfoSphere Guardium 8

The Most Complete Database Security Solution for Reducing Risk, Simplifying Compliance & Lowering Audit Costs

- Broadest platform support in the industry, including new System z capabilities
- Enhanced SAP monitoring for fraud
- First solution to monitor SharePoint repositories for sensitive data access (financials, designs, etc.)
- Robust risk mitigation & data-level security
  - Beyond monitoring to proactive access controls
  - Enhanced blocking: Quarantine & Fire-ID management
- Reduced cost & complexity of compliance
  - Centralized & automated, cross-platform policies
  - Advanced compliance workflow automation

InfoSphere Guardium 8 – Additional Enhancements

- Entitlement reporting
  - Unified solution for all supported DBMS platforms
- Vulnerability assessment enhancements
  - 500 new tests
  - Added tags for CVE standard
  - Based on industry-standard CIS Benchmark & DoD STIG
- Integration with Tivoli Security and Information Management (TSIEM)
  - Combines database monitoring information with log information from other sources (Windows, Unix, firewalls, IDS, etc.)
  - Enterprise-wide dashboard for security & compliance
- New DBMS platforms
  - PostgreSQL & Netezza
  - Complements previous support for IBM DB2 and Informix, Oracle, SQL Server, Sybase, MySQL, Teradata
- Numerous enhancements around scalability, usability & performance based on ongoing feedback from large-scale installations
  - E.g., automated on-boarding of new DBMS instances

Chosen by Leading Organizations Worldwide

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

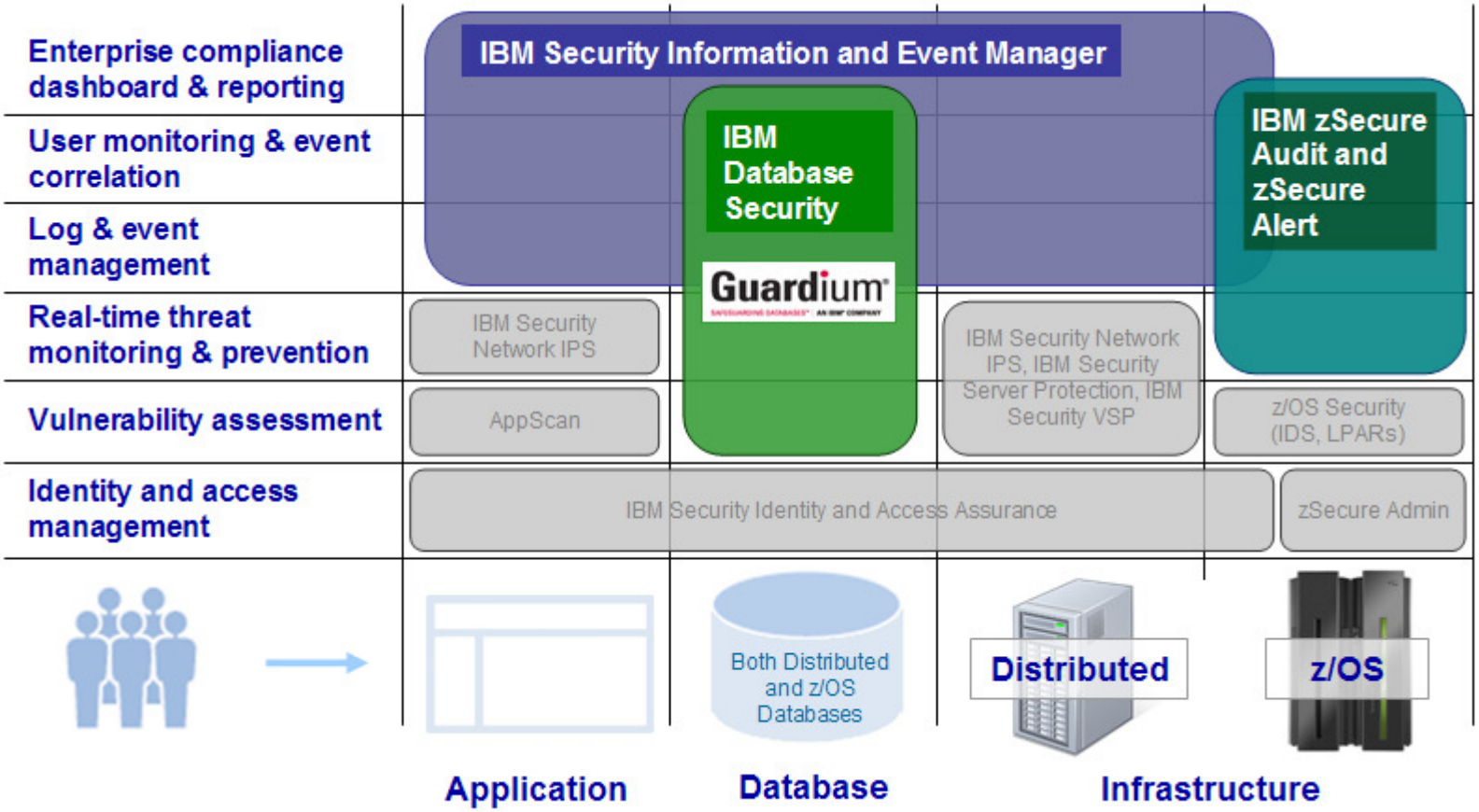
Thank You

Questions?

The IBM SecurityStudio Tackling the illusion of absolute security

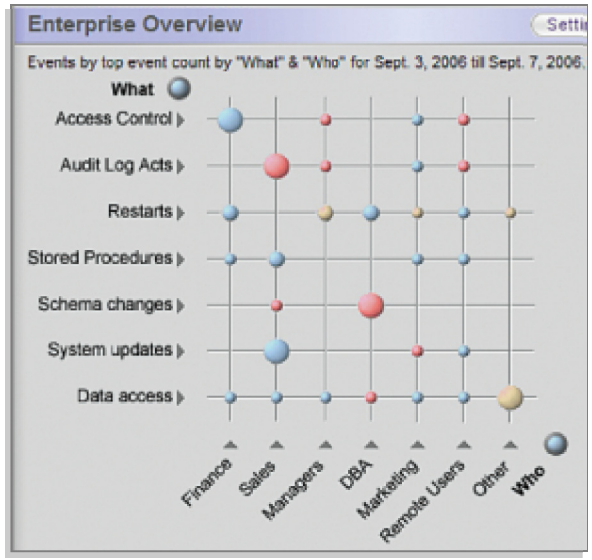
Appendix: TSIEM Overview

TSIEM, Guardium & zSecure are Complementary Products



Enforce Policy, Demonstrate Compliance, Manage Threats

TSIEM 2.0 – Value Proposition



- Primary focus on audit and compliance
- Privileged user activity monitoring is part of TSIEM DNA
  - Every event source ships with own definitions of privileged activity for that source
  - All relevant event sources have way to correlate real user names to make reports more meaningful
- Single model
  - W7 reduces the need for skilled staff
  - W7 produces reports auditors can understand
- In depth forensics to investigate issues
- Automation of processes improves overall reliability of reporting
- Integrated log management as a base
- Compliance management modules integrated into overall reporting
- Integration into Identity Management with closed loop auditing to help reduce risk and drive processes

Visibility Into Privileged Users & What They Did

User by Event type

Parameter Setup

What (event type)

- [x] Add : Privilege / Success
- [ ] Authenticate : User / Failure
- [x] Clear : Auditlog / Success
- [ ] Complete : Process / Success
- [x] Grant : Privilege / Failure
- [x] Grant : Privilege / Success
- [ ] Load : Module / Success
- [ ] Logoff : User / Success
- [ ] Logon : User / Failure
- [ ] Logon : User / Success
- [ ] Read : Access / Success
- [ ] Read : Config / Success
- [ ] Read : File / Success
- [ ] Receive : Message / Success
- [ ] Restart : System / Success
- [x] Start : Process / Success
- [ ] Start : Service / Success
- [x] Start : System / Success
- [ ] Stop : Service / Success
- [ ] Update : Parameter / Failure
- [ ] Use : Service / Success
- [ ] Use : Service / Success
- [x] Write : Config / Success
- [ ] Write : Log / Success

Submit Reset

Summary report

Who (Name)	Logonname	What (Event type)	#Events
Administrator	WINDOWS_NT01\Administrator	Add: Privilege / Success	294
Administrator	WINDOWS_NT01\Administrator	Clear: Auditlog / Success	1150
Administrator	WINDOWS_NT01\Administrator	Grant: Privilege / Success	334
Administrator	WINDOWS_NT01\Administrator	Start: System / Success	7
ROOT	LIN_SERV\ROOT	Add: Privilege / Success	5
ROOT	LIN_SERV\ROOT	Grant: Privilege / Success	7
ROOT	LIN_SERV\ROOT	Start: Process / Success	42
ROOT	LIN_SERV\ROOT	Start: System / Success	306
ROOT	LIN_SERV\ROOT	Write: Config / Success	42
System	NT AUTHORITY\SYSTEM	Start: Process / Success	494
System	NT AUTHORITY\SYSTEM	Start: System / Success	178
Michael Myers	WINDOWS_NT01\Managers\Michael076	Clear: Auditlog / Success	2
Michael Myers	WINDOWS_NT01\Managers\Michael076	Grant: Privilege / Failure	1
Eric Sanders	WINDOWS_NT01\Sales\Eric887	Start: Process / Success	18

1 2 3

Drill-Down by User & Event Type

User Audit

Parameter Setup

Who (source group)

- [x] Administrators
- [ ] Anonymous Accounts
- [ ] Anonymous Privileged Accounts
- [ ] Anonymous Regular Accounts
- [ ] Anonymous Users
- [ ] Banking Reservations
- [ ] Client Maintenance
- [ ] External Contractors
- [ ] FinAdmin Management
- [ ] FinAdmin Staff
- [ ] HK Management
- [ ] Human Rescources
- [x] IT
- [x] IT Admin
- [ ] Mail Account Services
- [ ] Mobile user
- [ ] Operations
- [ ] Operations Management
- [ ] Salary Administration
- [ ] Stock Holders
- [x] System
- [ ] Tele-worker
- [ ] Users
- [ ] Wealth Management

What (Event group)

- [x] Access Control
- [ ] Alerts
- [x] Alerts - High
- [ ] Alerts - Low
- [x] Attacks
- [x] Audit Log Actions
- [ ] Denied Access - Incoming
- [ ] Logon and logoff
- [ ] Logon failures
- [ ] Mail
- [ ] Network Services
- [ ] News
- [x] Password Changes
- [x] Remote Logon
- [ ] Restarts
- [x] Retrieve System Info
- [ ] System Actions
- [ ] System Processes
- [ ] System Services
- [x] System Updates
- [ ] User Actions - File
- [ ] User Actions - Process
- [x] Warnings

Submit Reset

Summary report

Who (Source group)	Logonname	Name	#Events
Administrators	WINDOWS_NT01\Administrator	Administrator	1545
Administrators	LIN_SERV\ROOT	ROOT	5644
Administrators	NT AUTHORITY\SYSTEM	System	1656
Administrators	WINDOWS_NT01\Admin\James075	James Patterson	1654
Administrators	WINDOWS_NT01\Admin\Tim812	Tim Doberty	4654
Administrators	WINDOWS_NT01\Admin\Maria073	Maria Devlon	3
Administrators	WINDOWS_NT01\Admin\Maria073	Marcus Jacobs	484

Drill-Down to Specific Users

User Summary of Ross Hikkings as MAINFR\Admin\Ross001

User information

Name	Ross Hikkings
Logonname	MAINFR\\Admin\\Ross001
#Events	15436
#Attention	245
#Exception	103
#Logon	21
#Logoff	20
#LogonFail	2
#Failure	65

Who

Who (Source group)
Administrators
Finance Admin

When

When (Period group)	**#Events**
Office Hours	10456
Week Evenings	3624
Weekend	1356

What on What

What (Event group)	**On What (Object group)**	**#Events**
Access Control	Financial Data	356
Audit Log Actions	Finacial Data	2
Alerts	Firewall	56
Alerts - High	Financial Data	6