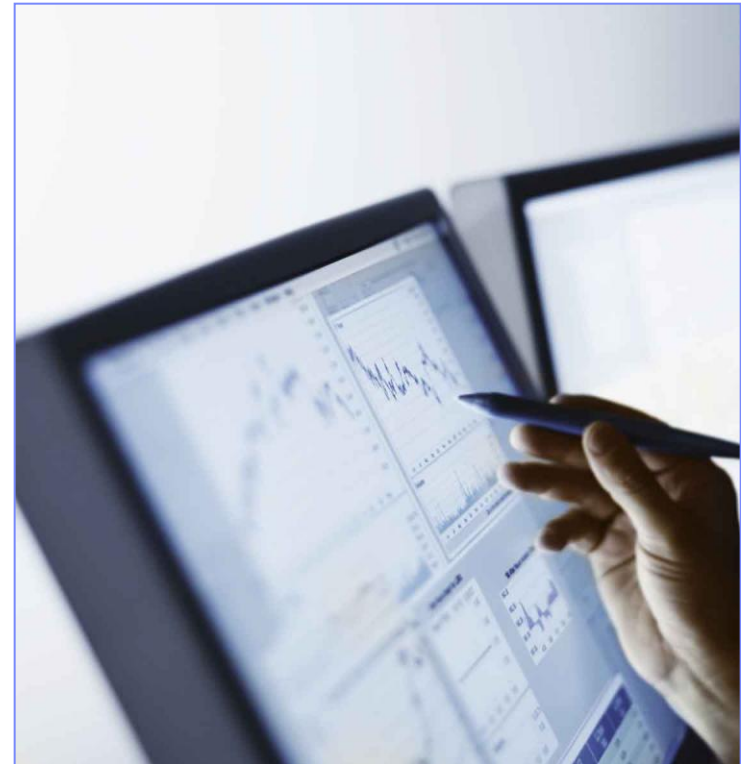


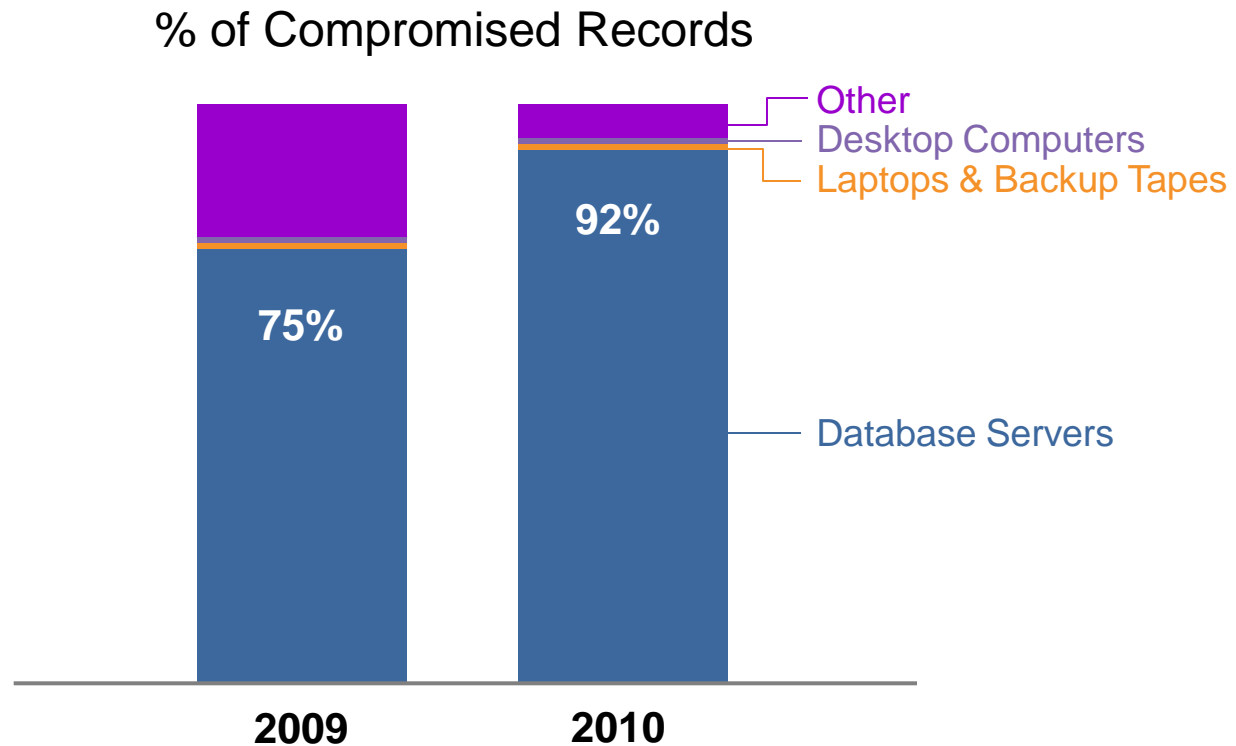
## A word cloud graphic featuring the text "Smarter software for a smarter planet" in a large, bold, blue font at the top. Below it, the words "Smarter software", "smarter planet", and "IBM" are repeated in various sizes and orientations (horizontal and vertical) in shades of green and blue. At the bottom right, the text "Information Management" is written in a large, bold, blue font. The background is white.

## What we'll discuss in this session

- Why database infrastructure protection is a top priority
- Issues with current approaches
- IBM's Database Activity Monitoring and Protect Solution
- Using InfoSphere Guardium to address a range of security and compliance needs
- Lessons from peer organizations
- Resources



## Database servers are the primary source of breached data



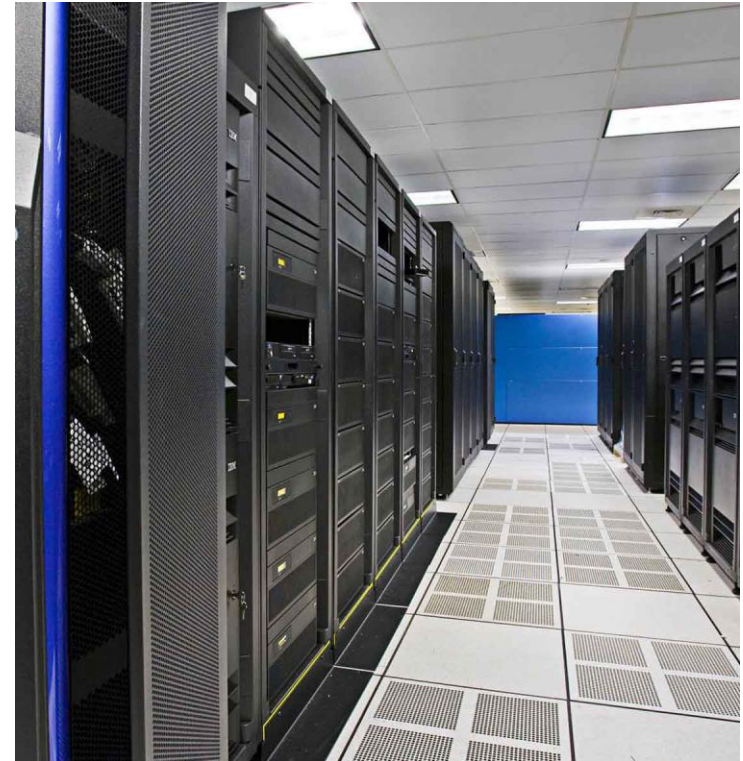
Sources: Verizon Business Data Breach Investigations Report 2009, 2010

“

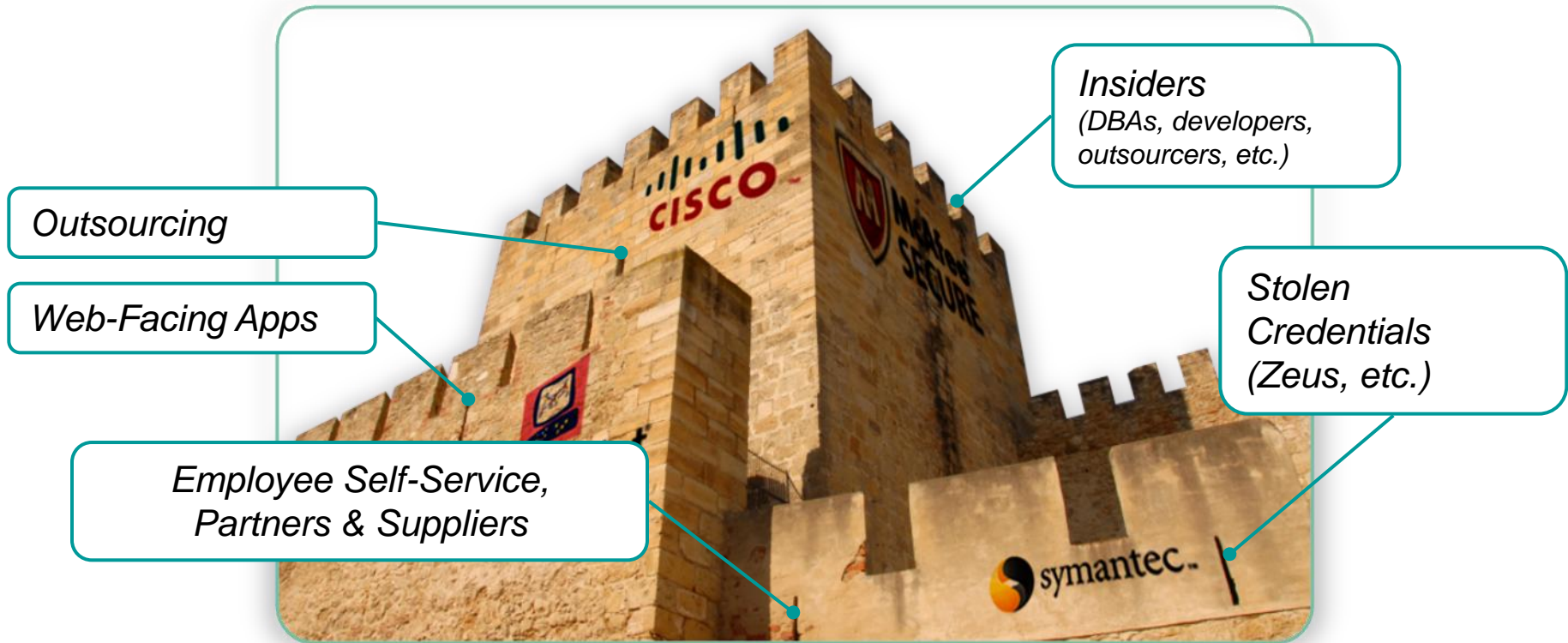
*Although much angst and security funding is given to **offline data, mobile devices, and end-user systems**, these assets are simply not a major point of compromise.*

## Why?

- Database servers contain your most valuable information
  - Financial records
  - Credit card and other account records
  - Patient records
  - Personally identifiable information
  - Customer data
- High volumes data
- Structured for easy to access



## 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

© 2010 IBM Corporation



# 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).



[http://www.darkreading.com/database\\_security/security/app-security/showArticle.jhtml?articleID=220300753](http://www.darkreading.com/database_security/security/app-security/showArticle.jhtml?articleID=220300753)

<http://www.ioug.org/BestPracticesSolutions/GSADownload/.../Default.aspx?...>

## The Enterprise Patching Issue

- Nearly half of companies lack a format 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*

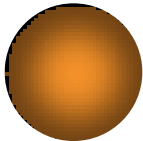

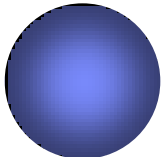






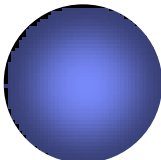




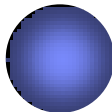
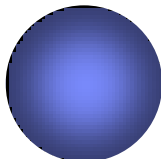


[http://www.darkreading.com/database\\_security](http://www.darkreading.com/database_security)

<http://www.securosis.com/projectquant>

[http://ioug.itconvergence.com/pls/apex/ESIG.download\\_my\\_file?p\\_file](http://ioug.itconvergence.com/pls/apex/ESIG.download_my_file?p_file)

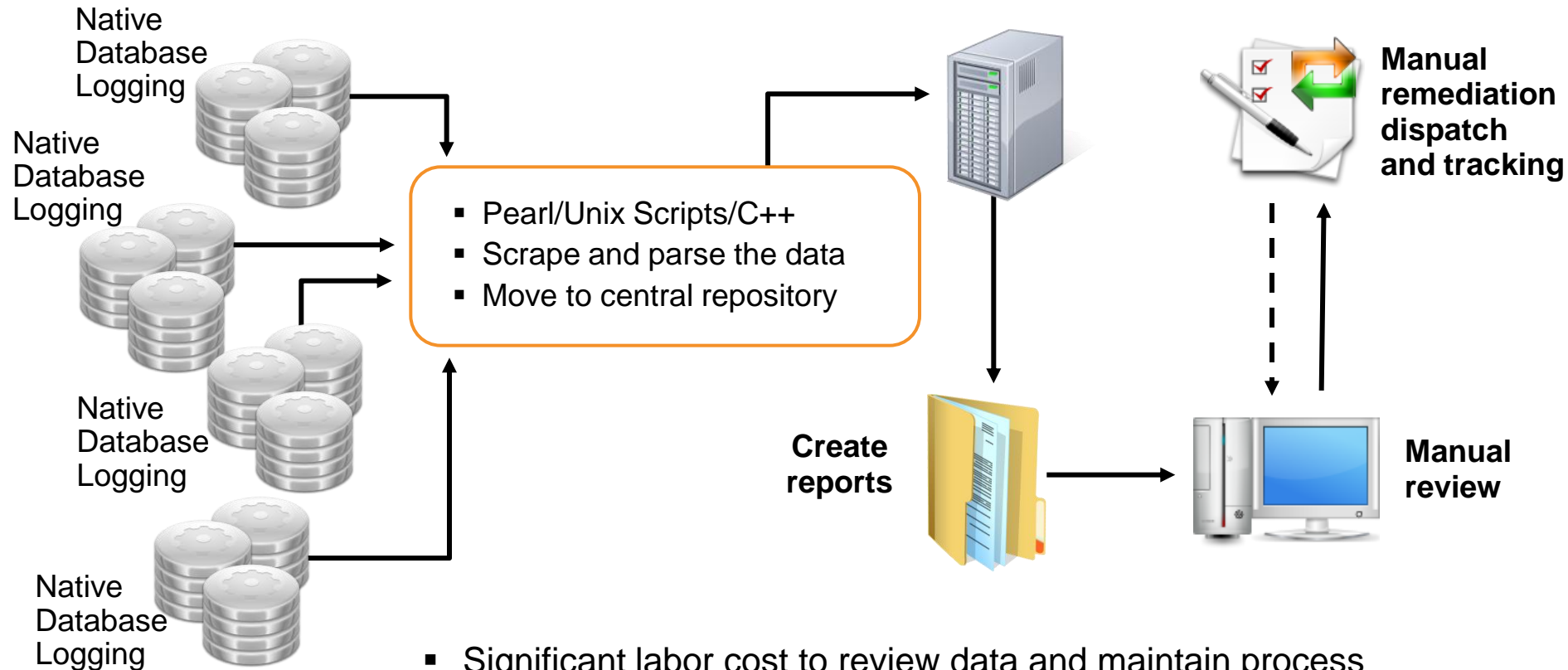
Compromises take days or more to discover in 79% of cases;  
and weeks or more to contain in over 53% of cases

Time span of events by percent of breaches

	Minutes	Hours	Days	Weeks	Months	Years/Never
Point of Entry to Compromise	 33%	 14%	 44%	 5%	 4%	 <1%
Compromise to Discovery	 <1%	 4%	 17%	 38%	 36%	 5%
Discovery to Containment	 <1%	 11%	 23%	 49%	 15%	 2%



## Typical home-grown solutions are costly and ineffective

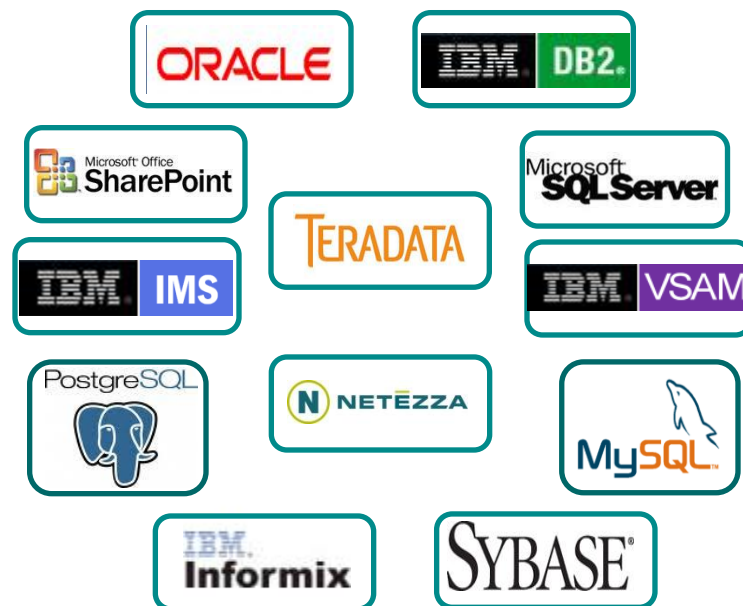
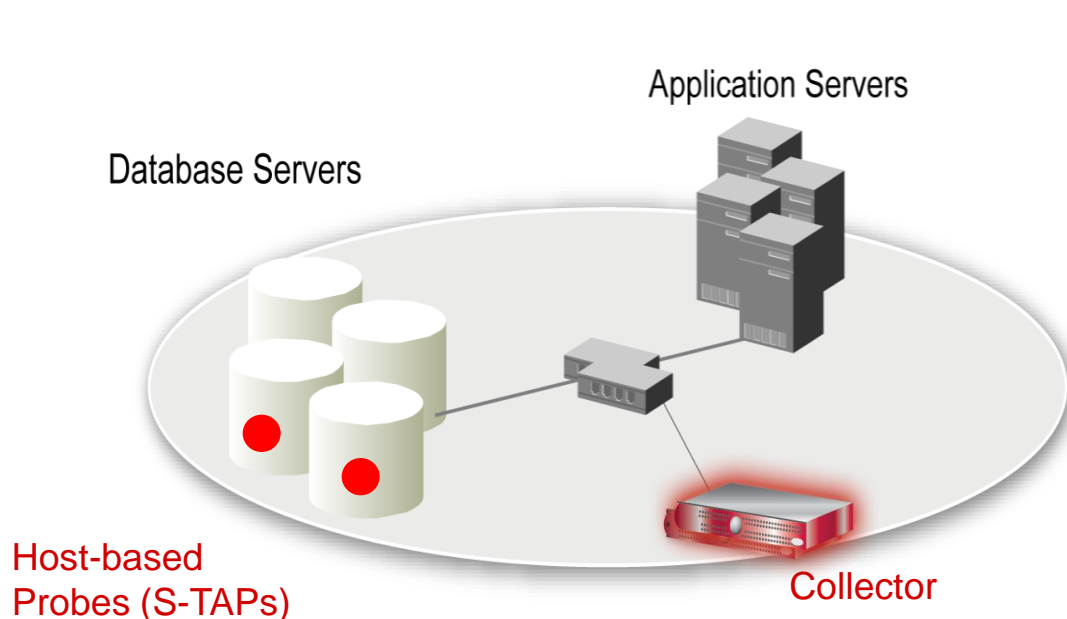


- Significant labor cost to review data and maintain process
- High performance impact on DBMS from native logging
- Not real time
- Does not meet auditor requirements for Separation of Duties
- Audit trail is not secure
- Inconsistent policies enterprise-wide

## 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

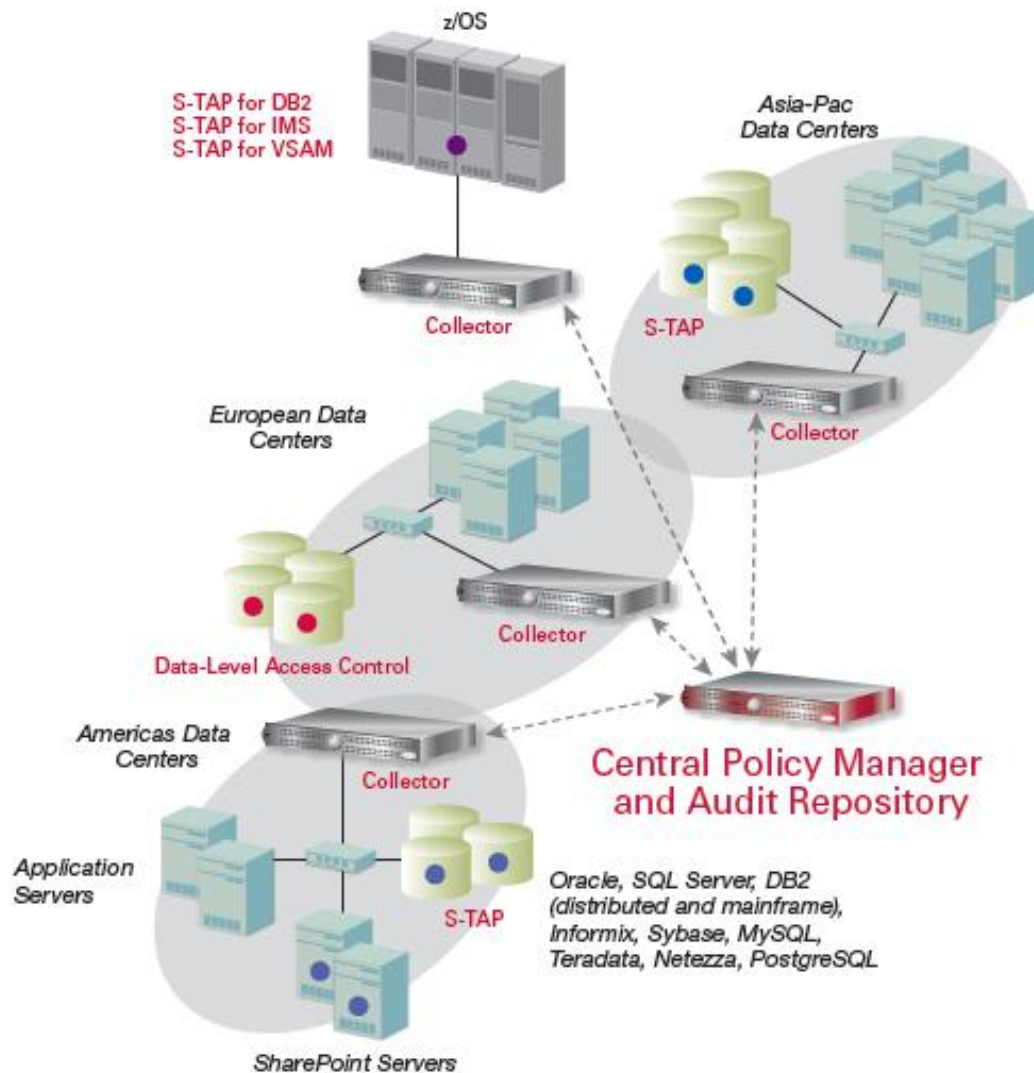
# Real time database monitoring and protection with InfoSphere Guardium



- No DBMS or application changes
- Does not rely on DBMS-resident logs that can easily be erased by attackers, rogue insiders
- 100% visibility including local DBA access
- Minimal performance impact

- Cross-DBMS solution
- Granular, real-time policies & auditing
  - *Who, what, when, how*
- Automated compliance reporting, sign-offs and escalations (financial regulations, PCI DSS, data privacy regulations, etc.)

## Scalable architecture supports application-specific and enterprise-wide deployments



# Addressing the full database security lifecycle





# Find uncataloged databases and identify sensitive data

Administration Console	Access Management	Tools	Daily Monitor	SQL Guard Monitor	Tap Monitor	Incident
SQL Count						
Session Count						
Logged Threshold Alerts						
Logged R/T Alerts						
Exception Count						
Dropped Requests						
TCP Exceptions						
Admin User Logins						
Databases by Type						
<b>Databases Discovered</b>						
Retrospective Report Requests						
Values Changed						
Throughput						

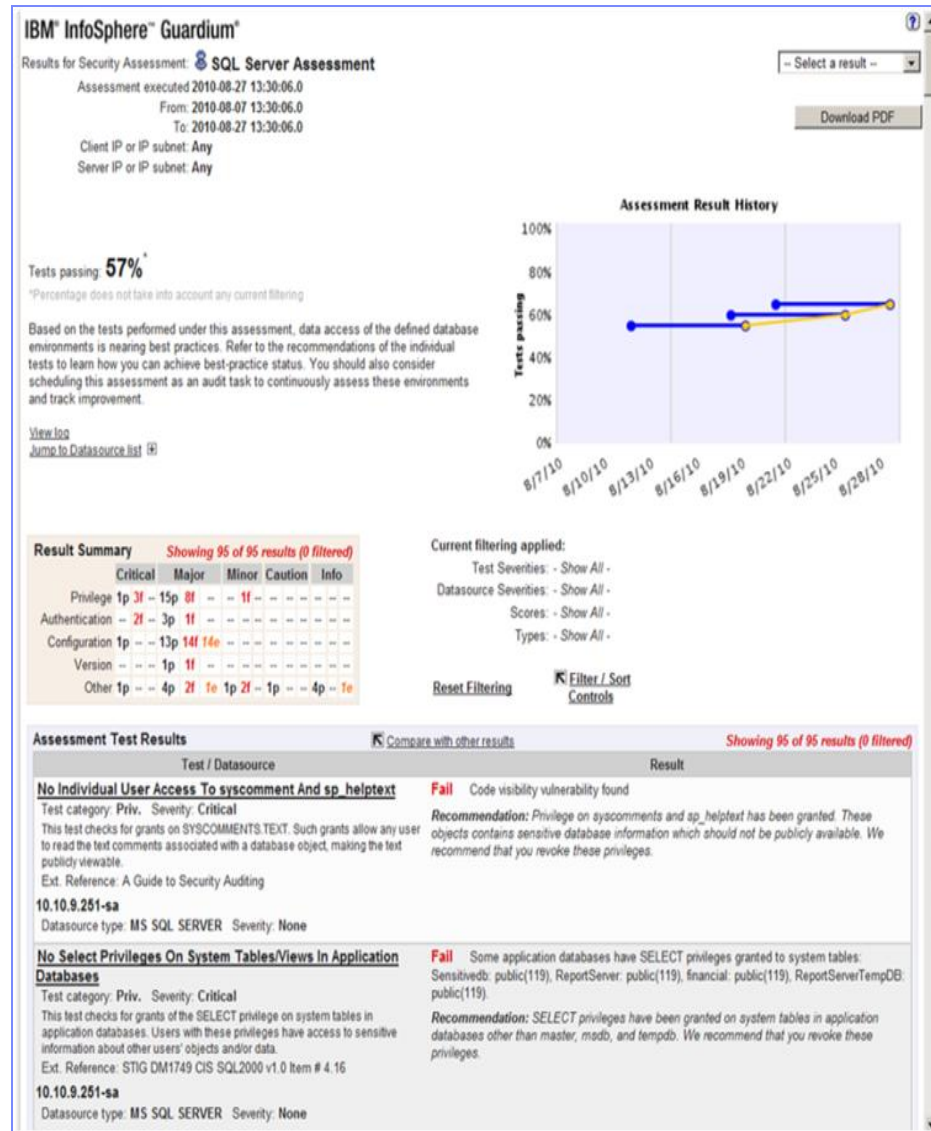
  

Databases Discovered						
Start Date: 2008-06-26 14:48:49 End Date: 2008-06-26 15:48:49						
Time Probed	Server IP	Server Host Name	DB Type	Port	Port Type	#
2008-06-26 15:31:00	10.10.9.253	10.10.9.253	Oracle	1521	tcp	1
2008-06-26 15:30:58	10.10.9.253	10.10.9.253	MSSQL	1433	tcp	1
2008-06-26 15:30:15	10.10.9.55	osprey	Oracle	1521	tcp	1
2008-06-26 15:30:15	10.10.9.55	osprey	Sybase	4200	tcp	1
2008-06-26 15:30:32	10.10.9.56	10.10.9.56	Oracle	1521	tcp	1
2008-06-26 15:30:58	10.10.9.56	10.10.9.56	DB2	50001	tcp	1

- Crawls the network to find uncataloged instances
- Four algorithms to identify sensitive data in databases
- Policy-based responsive actions
  - Alerts
  - Add to group of sensitive objects

Catalog	Schema	Table Name	Column Name	Rule Description	Comments	Classification Name	Category	Data Source Description
<input type="checkbox"/>	BANKAPP	CREDITCARD	CARDNUMBER	Send Alert	Date: Monday, July 21, 2008 6:30:07 PM EDT Datasource: ORACLE 10.10.9.56:1521 xe Object: TABLE BANKAPP.CREDITCARD VARCHAR2 (20) CARDNUMBER Category: 'PCI' Classification: 'Cardholder Data' Rule: Search For Data: Send Alert TABLE_TYPE='TABLE,VIEW', DATA_TYPE='TEXT', SEARCH_VALUE_PATTERN='10-9[4]{0-9}[4]{0-9}[4]- [0-9]{4}' Action: Send Alert: Send Alert Urgent Flag='false', Receiver='SYSLOG' Action: Log Policy Violation: Send Policy Violation Severity='10' Action: Add To Group Of Objects: add to group Object Group='PCI Cardholder Sensitive objects', Replace Group Content='false'	Cardholder Data	PCI	10-56-system

# Harden databases by identifying unpatched and misconfigured systems



Current Test Results

Prioritized Breakdown

Detailed Test Results

Result History

Filters and Sort Controls

Detailed Remediation Suggestions

# Eliminate inappropriate privileges

Cat.	Test Name	Datasource	P/F	Sev.	Reason
Priv.	<a href="#">Access To The UTL_FILE Package is restricted</a>	ORACLE: Oracle EE - Joe	Fail	Major	Found Exec UTL_FILE privilege granted to public  <i>Recommendation: Permissions to execute the UTL_FILE package have been granted to users other than DBAs. UTL_FILE allows users to access operating system files from Oracle, which may result in a security breach.</i>
Conf.	<a href="#">LOG_ARCHIVE_DUPLEX_DEST Set</a>	ORACLE: Oracle EE - Joe	Fail	Major	Parameter: 'LOG_ARCHIVE_DUPLEX_DEST' is not set.  <i>Recommendation: LOG_ARCHIVE_DUPLEX_DEST is not set. We recommend to set this parameter to a valid directory owned by Oracle set with owner and group read/write permissions only.</i>
Conf.	<a href="#">MAX_ENABLED_ROLES is not greater than 30</a>	ORACLE: Oracle EE - Joe	Fail	Major	Parameter: 'MAX_ENABLED_ROLES' with a value of '150' has been obsoleted for version 10.2.  <i>Recommendation: Max_enabled_roles is set to a value higher than 30. This parameter should be limited as much as possible (Typically SYS gets 20 roles by default)</i>
Priv.	<a href="#">No 'Catalog' Role Assignments</a>	ORACLE: Oracle EE - Joe	Fail	Major	Some users or roles other than predefined dba or roles have been granted default roles: SH, OLAPSYS, PERFSTAT, IX.  <i>Recommendation: Access to Data Dictionary and Catalog roles, 'SELECT_CATALOG_ROLE', 'OLAP_DBA', 'EXECUTE_CATALOG_ROLE', 'DELETE_CATALOG_ROLE', 'RECOVERY_CATALOG_OWNER' is granted to some users. We recommend restricting access to the Data Dictionary. Access to the Data Dictionary should be done using the V\$ views. 'SELECT_CATALOG_ROLE' may be granted to 'SYS', 'DBA', 'OEM_MONITOR', 'EXP_FULL_DATABASE', 'IMP_FULL_DATABASE', 'OLAP_DBA', 'OLAP_USER'. 'OLAP_DBA' may be granted to 'SYS', 'DBA', 'OLAPSYS'. 'EXECUTE_CATALOG_ROLE' may be granted to 'SYS', 'DBA', 'EXP_FULL_DATABASE', 'IMP_FULL_DATABASE'. 'DELETE_CATALOG_ROLE' may be granted to 'SYS', 'DBA'. 'RECOVERY_CATALOG_OWNER' may be granted to 'SYS'.</i>
Priv.	<a href="#">No Authority To Create Libraries</a>	ORACLE: Oracle EE - Joe	Fail	Major	Some users or roles without DBA or IMP_FULL_DATABASE authority have CREATE LIBRARY privileges: MDSYS, DMSYS, EXFSYS, ORDSYS, ORDPLUGINS, XDB.  <i>Recommendation: The CREATE LIBRARY (or CREATE ANY LIBRARY) privilege has been granted to some users. We recommend revoking this privilege unless it is absolutely necessary for a very minimal number of users to have the privilege. These privileges can be used to access the operating system, and they allow a user to load an operating system binary file and make calls to that binary's functions.</i>
Priv.	<a href="#">No Roles With The Admin Option</a>	ORACLE: Oracle EE - Joe	Fail	Major	Found roles granted WITH ADMIN option  <i>Recommendation: Roles have been granted with the admin option to roles or users other than DBA, SYS, and SYSTEM. When a role is grantable, a user can grant that role to other users. Since granting roles should be restricted, we recommend that you not grant roles with the GRANT option</i>

## Reduce the cost of managing user rights

- Provides a simple means of aggregating and understanding entitlement information
  - Scans and collects information on a scheduled basis, including group and role information
- Out-of-the box reports for common views
- Report writer for custom views
- Eliminates resource intensive and error prone processes of manually examining each database and stepping through roles

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

# Cross-platform policies and auditing for enterprise-wide deployment

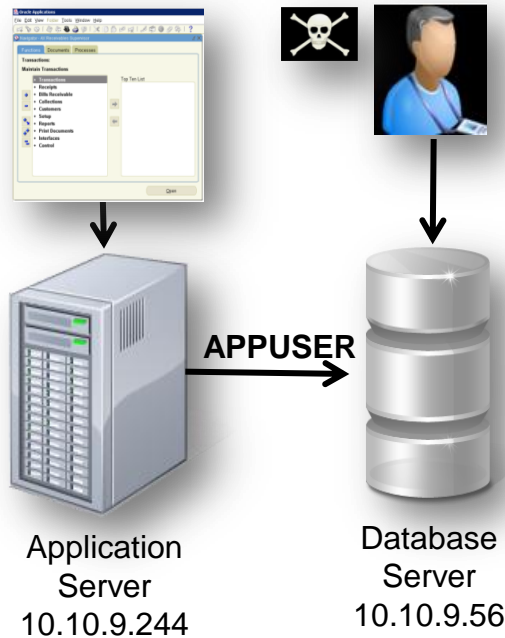
- Unified cross-platform policies easily defined
- Responsive actions defined within policies
- Single audit repository enables enterprise-wide compliance reporting and analytics

The screenshot displays the 'Access Rule Definition' window for 'Rule #2 of policy v8'. The rule is titled 'Granular Cross Platform Policy Rule' and is categorized under 'Security' with a 'HIGH' severity. The configuration is divided into several sections:

- Conditions:** A list of conditions on the left, each with a 'Not' checkbox and a selection field. The 'Server IP' condition is selected, and its value is '(Public) PCI Authorized Server IPs'. Other conditions include Client IP, Client MAC, Net Prtcl., DB Type, Svc. Name, DB Name, DB User, Client IP/Src, App. User, OS User, Src App., Field, Object, Command, Object/Cmd. Group, Object/Field Group, Pattern, XML Pattern, App Event Exists, App Event Values, Data Pattern, Time Period, Minimum Count, and Quarantine for.
- Actions:** A section at the bottom with a red box around the 'ALERT PER MATCH' action.
- Buttons:** 'Add Action', 'Back', and 'Save' buttons are located at the bottom right.



# A simple policy example: Preventing application bypass



**Rule #1 Description** non-App Source AppUser Connection

**Category** Security **Classification** Breach **Severity** MED

**Hot** ☐ **Server IP** / and/or **Group** Production Servers

**Hot** ☒ **Client IP** / and/or **Group** Authorized Client IPs

**Hot** ☐ **Client MAC** and/or **Net. Protocol** and/or **Group** -----

**Hot** ☐ **DB Name**

**Hot** ☐ **DB User** APPUSER

**Field Name**  
**Object** EmployeeTable  
**Command** Select

**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

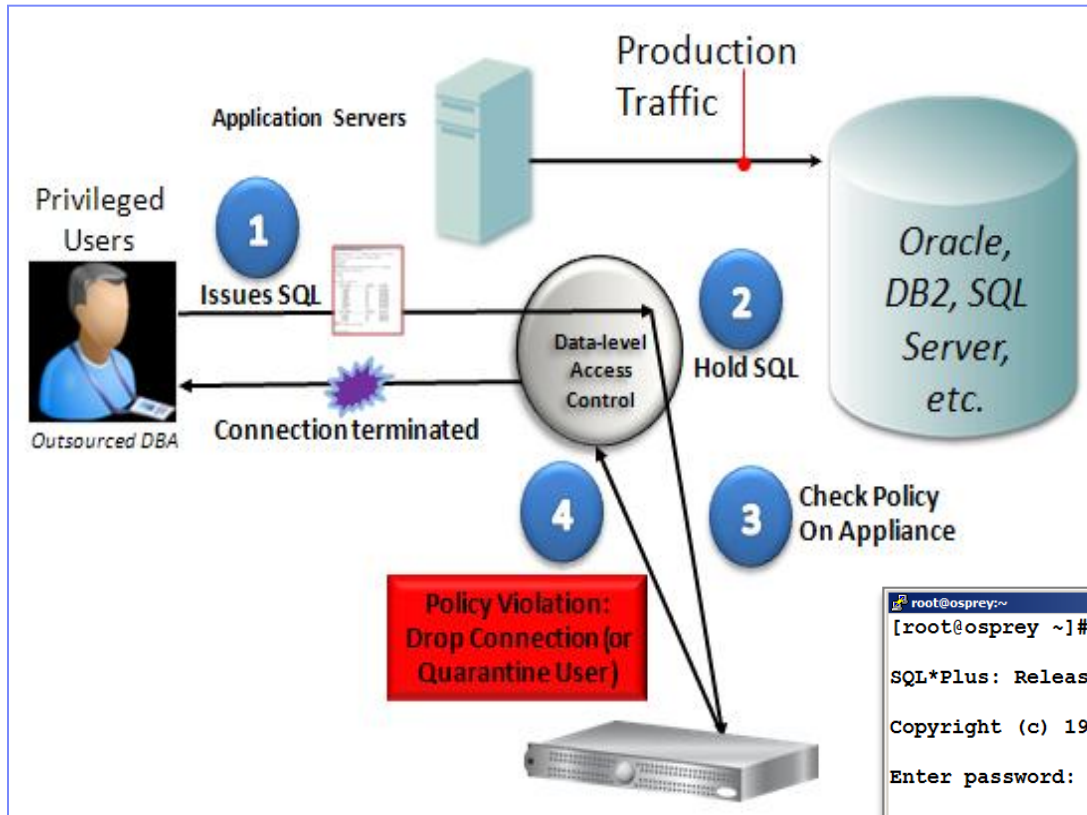
## Sample Alert

From: GuardiumAlert@guardium.com  
To: Marc Gamache  
Cc:  
Subject: (c1) SQLGUARD ALERT

Sent: Wed 4/15/2009 8:00 AM

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: INS DB Protocol Version: 3.8 DB User: APPUSER  
Application User Name  
Source Program: IDBC THIN CLIENT Authorization Code: 1 Request Type: SQL\_LANG Last Error:  
SQL: select \* from EmployeeTable

## Prevent policy violations in real-time (blocking)



- No database changes
- No application changes
- No network changes
- Without the performance or availability risks of an in-line database firewall

```
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
```

## Identify inappropriate use by authorized users

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

<u>DB User Name</u>	<u>Sql</u>	<u>Records</u>
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

# Automate oversight processes to ensure compliance and reduce operational costs

- Easily create custom processes by specifying unique combination of workflow steps, actions and users
  - Use case  
*Different oversight processes for financial servers than PCI servers*
- Supports automated execution of oversight processes on a report line item basis, maximizing efficiency without sacrificing security
  - Use case  
*Daily exception report contains 4 items I know about and have resolved, but one that needs detailed investigation. Send 3 on for sign-off; hold one*

**Event Type**

Existing Task Event Types

Event Type	First Status	Allowed Status
NA Store Daily PCI DSS Incident Workflo	Open	Approved, Not Approved, Open, Review state

**Edit Event Type Definition NA Store Daily PCI DSS Incident Workflo**

Description: NA Store Daily PCI DSS Incident Workflo

First Status: Open

**Allowed Status**

Available Status: Closed (Final)

Allowed Status: Approved (Final), Not Approved (Final), Open, Review state

**Defined Event Actions**

Event Action Description	Prior Status	Next Status	Sign-off
Under review	Open	Review state	<input type="checkbox"/>
Approved	Review state	Approved	<input checked="" type="checkbox"/>
Not approved	Review state	Not Approved	<input checked="" type="checkbox"/>

**Roles**

Roles have been assigned to this event type with status: Approved

Roles have been assigned to this event type with status: Open

Roles have been assigned to this event type with status: Not Approved

No roles have been assigned to this event type with status: Review state

Buttons: Cancel, Apply, New Event Type, Event Status

**Compliance Automation**

**Audit Process Definition**

Description: Daily PCI DSS Incident: Review

Active: ☒ There is no schedule associated with this process

Archive Results: ☐

Keep for a minimum of: 365 days or 0 runs

CSV/CEF File Label: Daily\_PCI\_DSS\_Incident\_

Email Subject: Daily PCI DSS Incidents for Remediation and Sign-off

Buttons: View, Run Once Now, Modify Schedule...

**Receiver Table**

Receiver	Action Req.	To-Do List	Email Notif.	Cont. Appv. if Empty
Payment Card DB Admin (Ernst Potherfeldt)	Review Sign	<input checked="" type="checkbox"/>	No Link Full Results	<input checked="" type="checkbox"/>
Retail InfoSec (Max Dufresne)	Review Sign	<input checked="" type="checkbox"/>	No Link Full Results	<input checked="" type="checkbox"/>

**Add Receiver**

Receiver name: Search users

Action Required: Review Sign

To-Do List: Add

Email Notification: None Link Only Full Results

Continuous: ☒

Approve if Empty: Yes

Buttons: Add

**Audit Tasks**

Report: Daily PCI DSS Incident Report [Policy Violations Details] [NOW -1 DAY to NOW]

Buttons: Add Audit Task

# InfoSphere Guardium allows you to protect your most valuable information

Continuously monitor access to high-value databases to:



## 1. Prevent data breaches

Mitigate external and internal threats



## 2. Ensure the integrity of sensitive data

Prevent unauthorized changes to sensitive data or structures



## 3. Reduce cost of compliance

Automate and centralize controls

1. Across PCI DSS, data privacy regulations, HIPAA/HITECH, ...
2. Across databases and applications

Simplify processes



## 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

## Can You Afford a DAM Solution?



*Commissioned Forrester Consulting Case Study*

- **Who:** F500 consumer food manufacturer (\$15B revenue)
- **Need:** Secure SAP and Siebel data for SOX
  - Enforce change controls & implement consistent auditing across platform
- **Environment:**
  - SAP, Siebel, Manugistics, IT2 + 21 other Key Financial Systems (KFS)
  - Oracle & IBM DB2 on AIX; SQL Server on Windows
- **Results:** 239% ROI & 5.9 months payback, plus:
  - **Proactive security:** Real-time alert when changes made to critical tables
  - **Simplified compliance:** Passed 4 audits (internal & external)
    - “The ability to associate changes with a ticket number makes our job a lot easier ... which is something the auditors ask about.” [Lead Security Analyst]
  - **Strategic focus on data security**
    - “There’s a new and sharper focus on database security within the IT organization. Security is more top-of-mind among IT operations people and other staff such as developers.”

## PCI Compliance for McAfee.com

- **Who:** World's largest dedicated security company
- **Need:** Safeguard millions of PCI transactions
  - Maintain strict SLAs with ISP customers (Comcast, COX,
  - Automate PCI controls
- **Environment:** Guardium deployed in less than 48 hours
  - Multiple data centers; clustered databases
  - Integrated with ArcSight SIEM
  - Expanding coverage to SAP systems for SOX
- **Previous Solution:** Central database audit repository with native DBMS logs
  - Massive data volumes; performance & reliability issues; SOD issues
- **Results:**
  - *“McAfee needed a solution with continuous real-time visibility into all sensitive cardholder data – in order to quickly spot unauthorized activity and comply with PCI-DSS – but given our significant transaction volumes, performance and reliability considerations were crucial.”*
  - *“We were initially using a database auditing solution that collected information from native DBMS logs and stored it in an audit repository, but granular logging significantly impacted our database servers and the audit repository was simply unable to handle the massive transaction volume generated by our McAfee.com environment.”*



# Implementing automated and centralized controls yields global manufacturer 239% ROI

## Challenge

- **Who:** F500 consumer food manufacturer (\$15B revenue)
- **Need:** Secure SAP and Siebel data
  - Enforce change controls & implement consistent auditing across platforms
- **Environment:**
  - SAP, Siebel, Manugistics, IT2 + 21 other key financial systems
  - Oracle and IBM DB2 on AIX; SQL Server on Windows



Commissioned Forrester  
Consulting Case Study

## Business Benefits

- **Results: 239% ROI and 5.9 months payback, plus:**
- Proactive security: Real-time alert when changes made to critical tables
- Simplified compliance: Passed 4 audits (internal and external)
  - "The ability to associate changes with a ticket number makes our job a lot easier ... which is something the auditors ask about."*  
[Lead Security Analyst]
- Strategic focus on data security
  - "There's a new and sharper focus on database security within the IT organization. Security is more top-of-mind among IT operations people and other staff such as developers."*

# Simplifying enterprise security for Dell

## Challenge

- **Who:** Leading global supplier of PCs and technology products. \$61B in revenue; 257th in Global Fortune 500
- **Need:**
  - Improve database security for SOX, PCI and SAS70
  - Simplify and automate compliance controls
- **Environment:**
  - Oracle and 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

## Business Benefits

- **Results:** Automated compliance reporting; real-time alerting; centralized cross-DBMS policies; closed-loop change control with Remedy integration
- InfoSphere Guardium *“successfully met Dell’s requirements without causing outages to any databases; produced a significant reduction in auditing overhead in databases.”*

## Solution

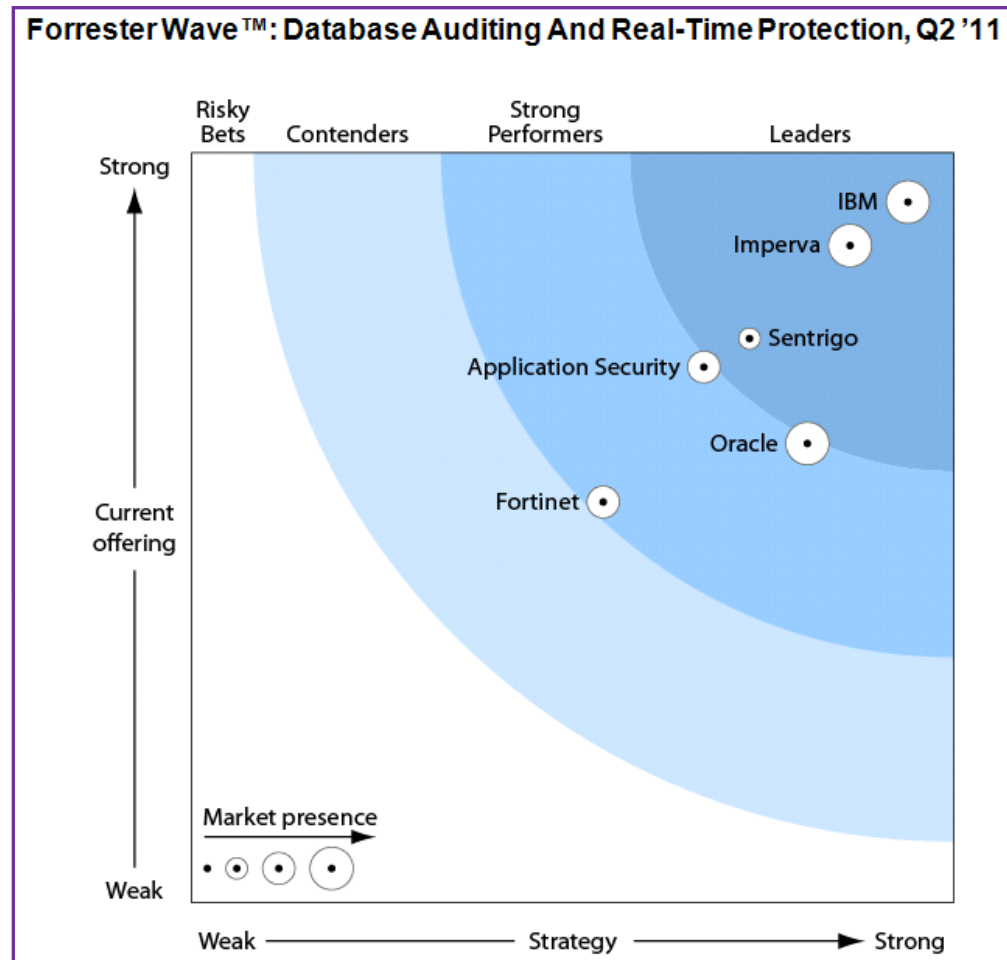
- **InfoSphere Guardium Deployment:**
  - Phase 1: Deployed to 300 DB servers in 10 data centers (in 12 weeks)
  - Phase 2: Deployed to additional 725 database servers



## Chosen by over 500 leading organizations worldwide



## InfoSphere Guardium continues to demonstrate its 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 judgment 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”	<b><i>The Evaluation Process</i></b> <ul style="list-style-type: none"><li>▪ 6 of the top vendors evaluated</li><li>▪ Examined past research</li><li>▪ Customer reference calls</li><li>▪ Conducted user needs assessments</li><li>▪ Conducted vendor and expert interviews</li><li>▪ Examined product demos</li><li>▪ Conducted lab evaluations</li><li>▪ 147 evaluation criteria</li></ul>
Awarded highest score in overall “Strategy”	
Awarded highest score in evaluation of “Current Offering”	
Achieved highest score possible in 8 out of 16 high-level scored categories	
Achieved the top ranking in 7 high-level categories; tied for top ranking in 1 category	
Evaluation based on v7, v8 introduced weeks after cutoff	

**“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 ”**

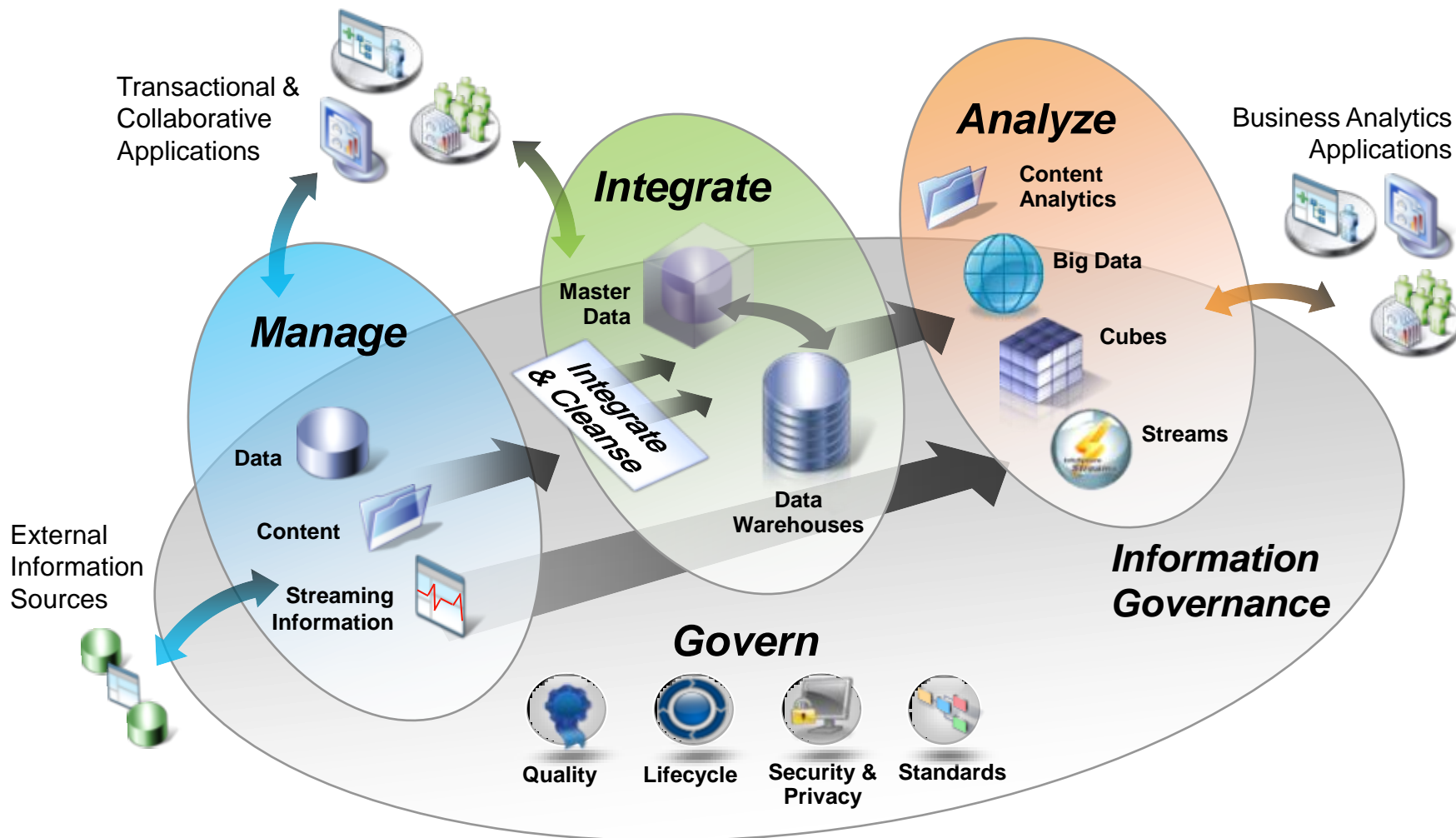
**“InfoSphere Guardium offers support for almost any of the features one might find in an auditing and real-time protection solution”**

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

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

***“IBM’s acquisition of Guardium in 2009 changed everything, making IBM one of the leading players.”***

# Mastering information across the Information Supply Chain



**Trusted ♦ Relevant ♦ Governed**



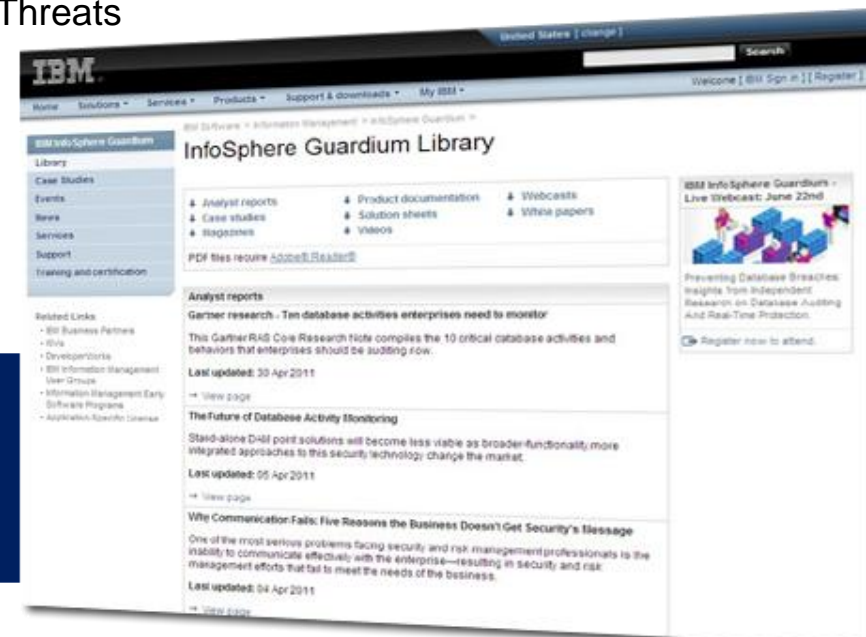
## Summary

- In the current environment, a means for securing high-value databases and validating compliance is a necessity
- Traditional log management, SIEM and DLP solutions are insufficient to secure sensitive databases
  - No real-time monitoring at data level to detect unauthorized activities
  - Native logging/auditing require database changes and impact performance
  - No knowledge of DBMS commands, vulnerabilities and structures
  - Inability to detect fraud at application layer
- InfoSphere Guardium is the most widely-deployed solution, with ongoing feedback from the most demanding data center environments worldwide
  - Scalable enterprise architecture
  - Broad heterogeneous support
  - Complete visibility and granular control
  - Deep automation to reduce workload and total cost of operations
  - Holistic approach to security and compliance

## Broad array of additional resources available

- Analyst reports
  - Forrester Wave (link also located on top right corner of Guardium page)
  - Gartner: 10 Database Activities You Need to Monitor
  - Forrester: Your Enterprise Database Security Strategy
  - Forrester: Look Beyond Database Auditing to Improve Security, Audit Visibility and Real-Time Protection
- Technical on-demand webinars
  - Vulnerability Assessment, Protecting Against Top 5 Threats
  - Verizon: Data Breach Investigations Report
  - Forrester: Best Practices for DB Security and Compliance
- Chapter downloads of database security texts
  - Implementing Database Security and Auditing
  - HOWTO Secure and Audit Oracle 10g and 11g

**Go to [ibm.com](http://ibm.com) and search for InfoSphere Guardium; look for the “Library” tab in the top left corner.**



## Broadest platform support in the industry

Supported Platforms	Supported Versions
Oracle	8i, 9i, 10g (r1, r2), 11g, 11gr2
Oracle (ASO, SSL)	9i, 10g(r1,r2), 11g
Microsoft SQL Server	2000, 2005, 2008
Microsoft SharePoint	2007, 2010
IBM DB2 (Linux, Unix, Linux for System z)	9.1, 9.5, 9.7
IBM DB2 (Windows)	9.1, 9.5, 9.7
IBM pureScale	9.8
IBM DB2 for z/OS	8.1, 9.1, 10.1
IBM IMS	9, 10, 11, 12
IBM VSAM	See OS support chart
IBM DB2 for iSeries	V5R2, V5R3, V5R4, V6R1
IBM Informix	7, 9, 10,11,11.5, 11.7
MySQL and MySQL Cluster	4.1, 5.0, 5.1
Sybase ASE	12, 15, 15.5
Sybase IQ	12.6, 12.7, 15
Netezza	4.5, 4.6, 4.6.8, 5.0, 6.0
PostgreSQL	8,9
Teradata	6.X, 12, 13, 13.1
FTP	