IBM Information Governance Security Software Overview for Innovapost

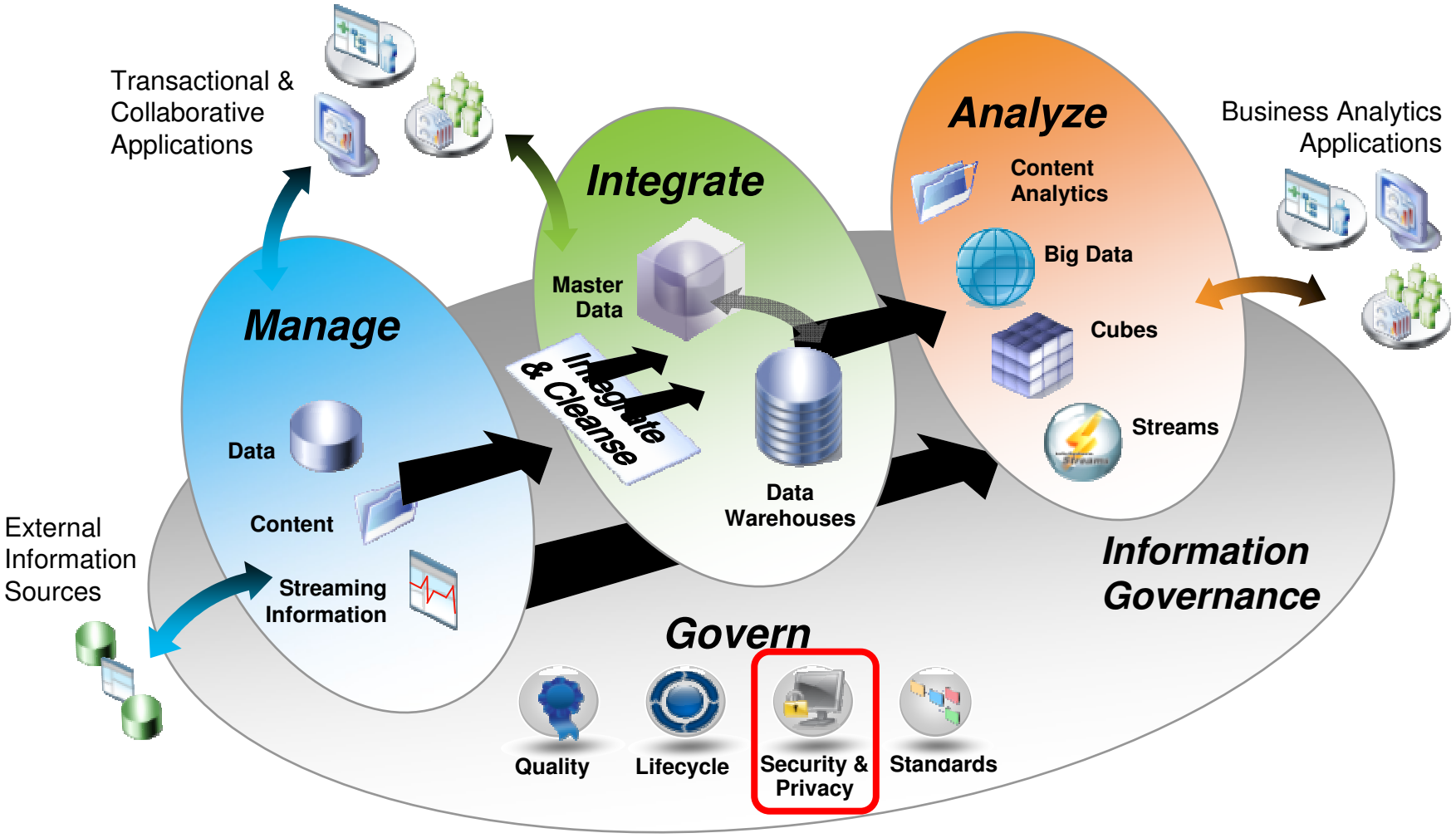
June 14, 2013

Ken Lee, kklee@ca.ibm.com

Agenda

- Introduction
- IBM InfoSphere Discovery
- IBM InfoSphere Guardium Database Activity Monitor
- IBM InfoSphere Guardium Data Encryption
- IBM InfoSphere Guardium Data Redaction
- IBM InfoSphere Optim Data Privacy

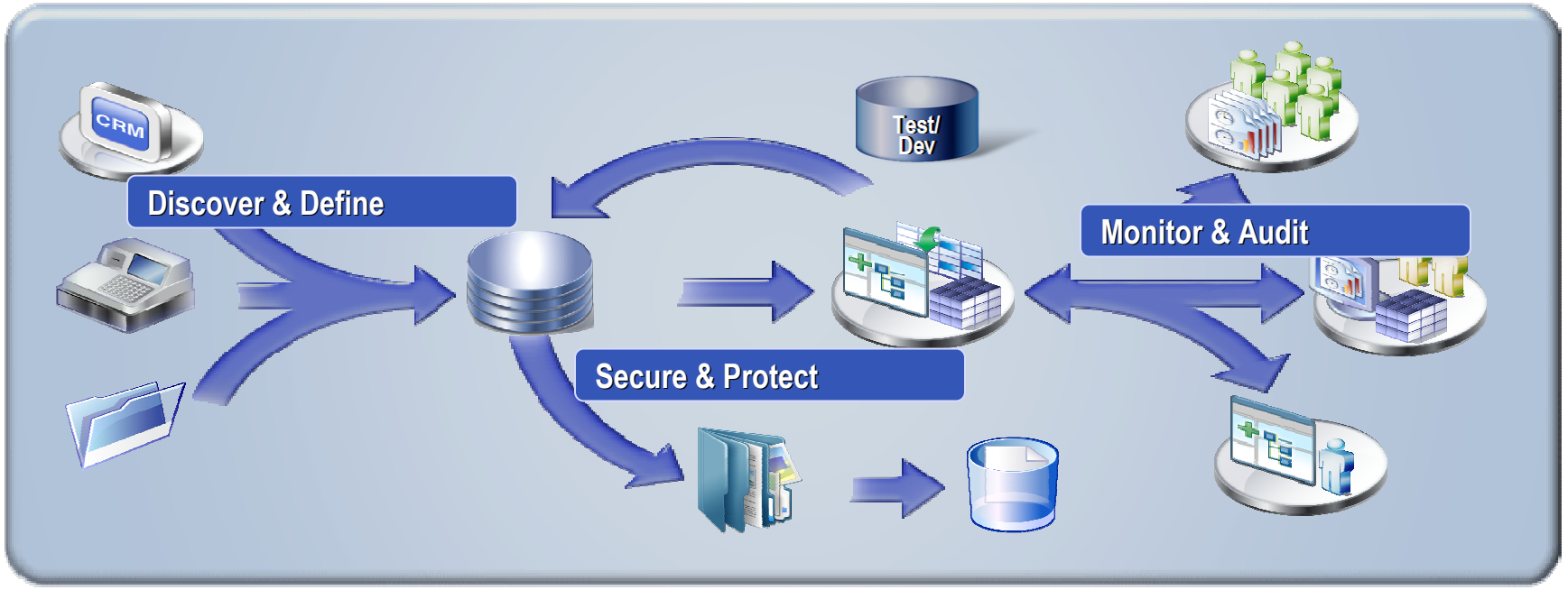
Mastering information across the Information Supply Chain



Trusted ◆ Relevant ◆ Governed

Securing and Protecting Your Information Supply Chain

- **Understanding the "what & where" of enterprise data**
- **Protecting the data across the enterprise, both internal and external threats**
- **Knowing who's accessing your data when, how and why**
- **Monitoring and reporting on database access for audit purposes**



Requirements to manage security & protection of data

Information Governance Core Disciplines
Security and Privacy

Understand & Define	Secure & Protect	Monitor & Audit
Discover where sensitive data resides	Protect enterprise data from both authorized & unauthorized access	Audit and report for compliance
Classify & define data types	Safeguard sensitive data in documents	Monitor and enforce database access
Define policies & metrics	De-identify confidential data in non-production environments	Assess database vulnerabilities

Data Stewards *"I need to understand my data better to determine what needs to be secured."*

Chief Compliance Officer *"We need a comprehensive strategy to protect structured & unstructured data in all enterprise environments & ensure we can detect a potential breach before it occurs."*

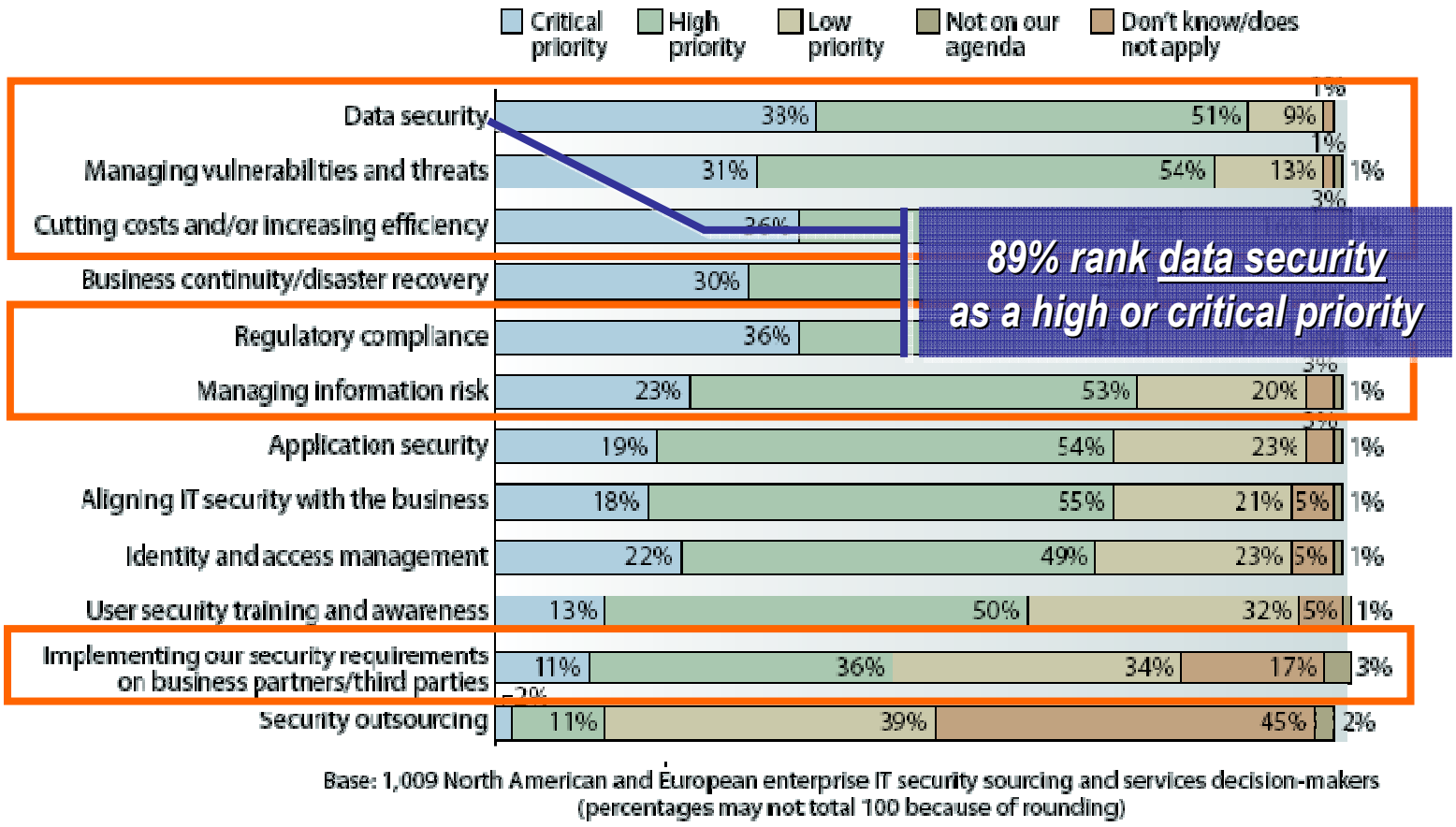
Chief Security Officer *"I need common security policies for my enterprise."*

InfoSphere Security and Privacy Solutions

- **InfoSphere Discovery**
  - Identify and document enterprise data relationships including the location of sensitive information
- **InfoSphere Guardium Database Activity Monitor**
  - Database Activity Monitoring & Auditing
  - Know who is accessing your data in real-time and meet business security audits
- **InfoSphere Guardium Data Encryption**
  - Encrypt sensitive data and provide access for the right user
- **InfoSphere Guardium Data Redaction**
  - Protect sensitive unstructured information in documents from unintentional disclosure
- **InfoSphere Optim Test Data Management and Data Privacy**
  - Mask private information across non-production environments
  - Protect sensitive information close to the source or as its being extracted

Top IT Security Initiatives

"Which of the following are likely to be your organization's top IT security priorities over the next 12 months?"

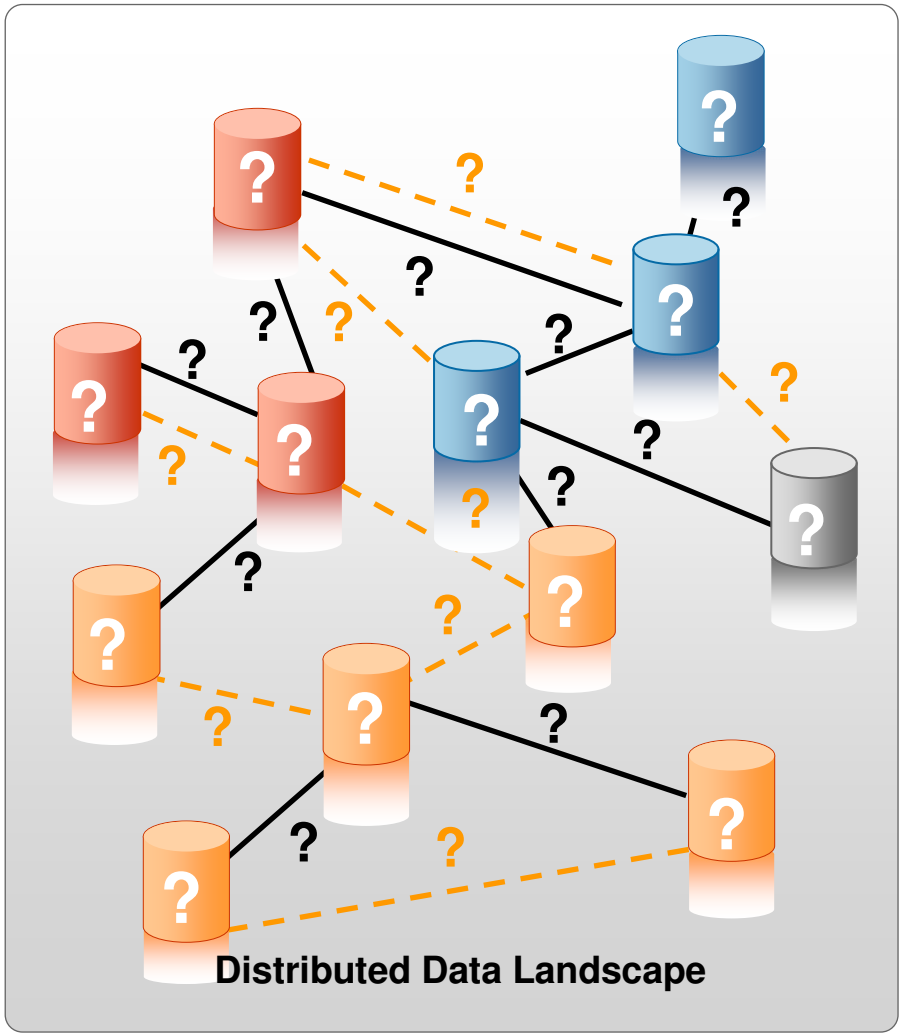


Base: 1,009 North American and European enterprise IT security sourcing and services decision-makers
(percentages may not total 100 because of rounding)

Source: Forrester Research, Inc. Jonathan Penn, "The State Of Enterprise IT Security And Emerging Trends: 2009 To 2010" – January 2010

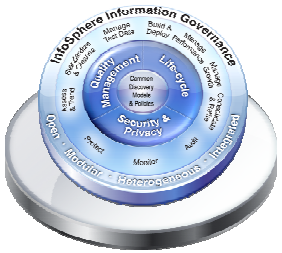
InfoSphere Discovery

You can't manage what you don't understand



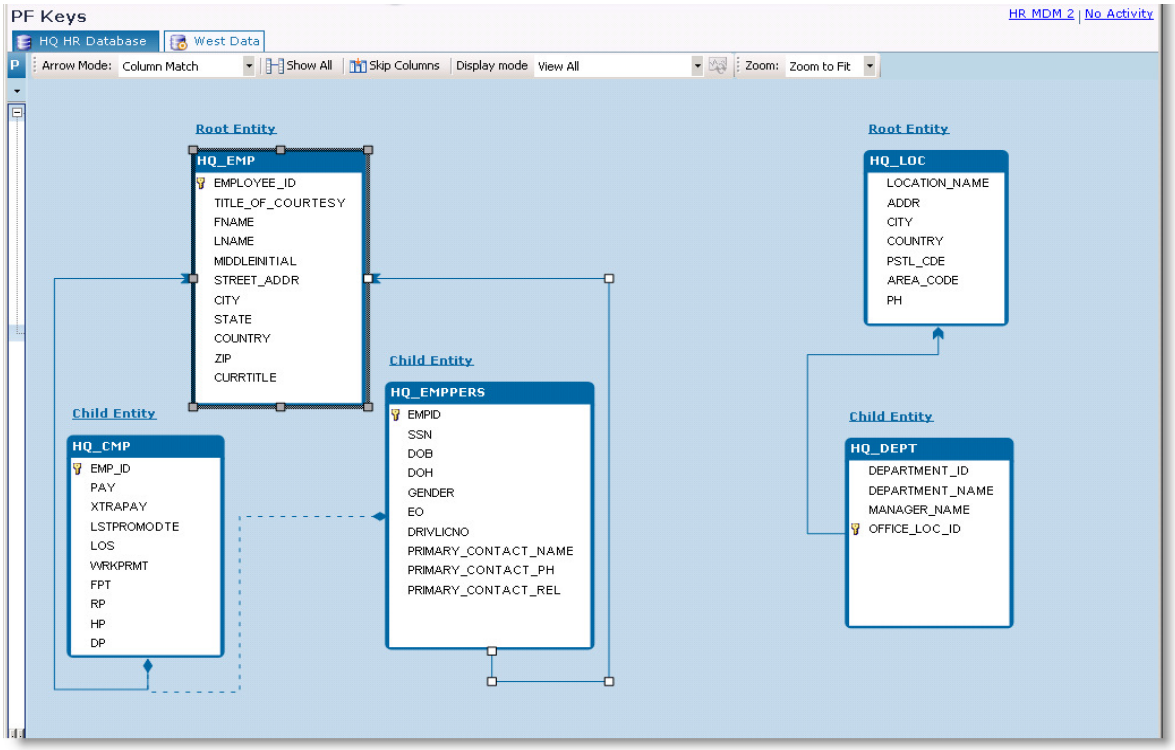
- **Data can be distributed over multiple applications, databases and platforms**
  - Where are those databases located?
  - Who can access the data?
- **Complex, poorly documented data relationships**
  - Which data is sensitive, and which can be shared?
  - Whole and partial sensitive data elements can be found in hundreds of tables and fields
- **Data relationships not understood because:**
  - Corporate memory is poor
  - Documentation is poor or nonexistent
  - Logical relationships (enforced through application logic or business rules) are hidden

IBM InfoSphere Discovery



Discovery

Accelerate project deployment by automating discovery of your distributed data landscape



Discovery supports analysis of data on distributed platforms (LUW), z/OS and flat files.

Note: Additional application specific solutions available for SAP, Oracle eBiz, Siebel, JDEdwards, PeopleSoft

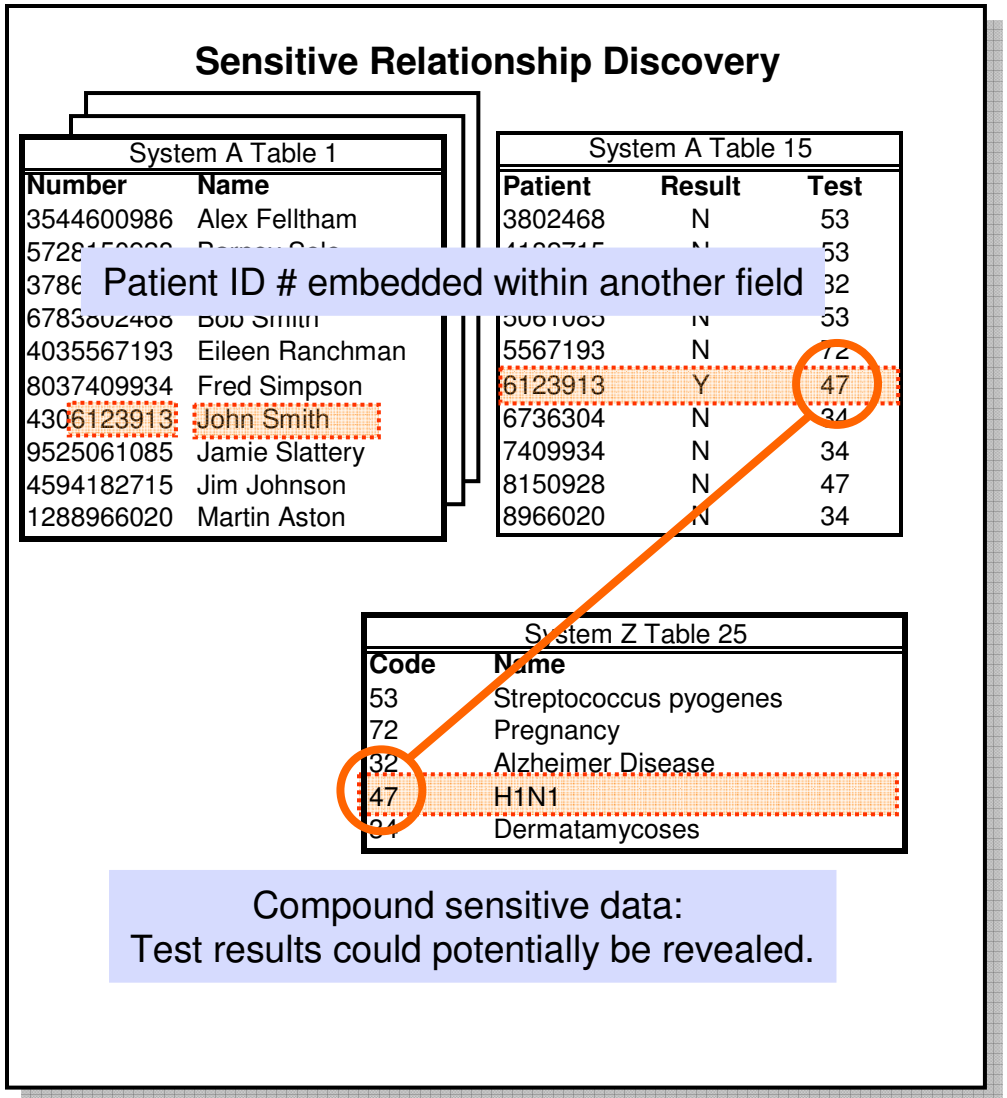
Requirements

- Identify hidden sensitive data requiring protection
- Define business objects for securing sensitive data
- Discover data transformation rules and heterogeneous relationships to secure data

Benefits

- Minimize risk of breaches by implementing consistent security controls
- Automate manual activities to minimize cost and time while maximizing quality
- Business insight into data relationships reduces project risk

Discover How Data is Related and Where Sensitive Data May Be Hidden



- **Relationships and sensitive data can't always be found just by a simple data scan**
  - Sensitive data can be embedded within a field
  - Sensitive data could be revealed through relationships across fields & systems
- **When dealing with hundreds of tables and millions of rows, this search is complex – you need the right solution**

InfoSphere Guardium Database Activity Monitor

Sony Data Breach Exposes 100 Million Customers to Years of Identity-Theft Risk – Costs Skyrocket Beyond $170 Million

Japan

- **Hackers exploited a known security vulnerability to gain access to** 77 million **PlayStation Network and Qriocity user names, addresses, gender, birth dates and other information in mid-April 2011.**
- **Hackers also gained access to** 23,400 credit card and debit records **from non-U.S. customers and the personal account information of** 24.6 million **account holders from a separate unit, Sony Online Entertainment.**
- **The** attackers may have stolen customer names, birth dates, and potentially the mother's maiden name**. These are all the things used to check a customer's identity, and that can be used to falsify it.**
- **Sony took a** $179 Million **charge in their latest quarter, but has stated "In addition, in connection with the data breach,** class action lawsuits have been filed against Sony **and certain of its subsidiaries and regulatory inquiries have begun; however, those are all at a preliminary stage, so we are not able to include the possible outcome of any of them in our results forecast for the fiscal year ending March 2012 at this moment."**

Data is the key target for security breaches…..
… and Database Servers Are The Primary Source of Breached Data

Table 10. Compromised assets by percent of breaches and percent of records*

Type	Category	All Orgs		Larger Orgs	
POS server (store controller)	Servers	50%	1%	2%	<1%
POS terminal	User devices	35%	<1%	2%	<1%
Desktop/Workstation	User devices	18%	34%	12%	36%
Automated Teller Machine (ATM)	User devices	8%	<1%	13%	<1%
Web/application server	Servers	6%	80%	33%	82%
Database server	Servers	6%	96%	33%	98%
Regular employee/end-user	People	3%	1%	5%	<1%
Mail server	Servers	3%	2%	10%	2%
Payment card (credit, debit, etc.)	Offline data	3%	<1%	0%	<1%
Cashier/Teller/Waiter	People	2%	<1%	2%	<1%
Pay at the Pump terminal	User devices	2%	<1%	0%	<1%
File server	Servers	1%	<1%	5%	<1%
Laptop/Netbook	User devices	1%	<1%	5%	<1%
Remote access server	Servers	1%	<1%	7%	<1%
Call Center Staff	People	1%	<1%	7%	<1%

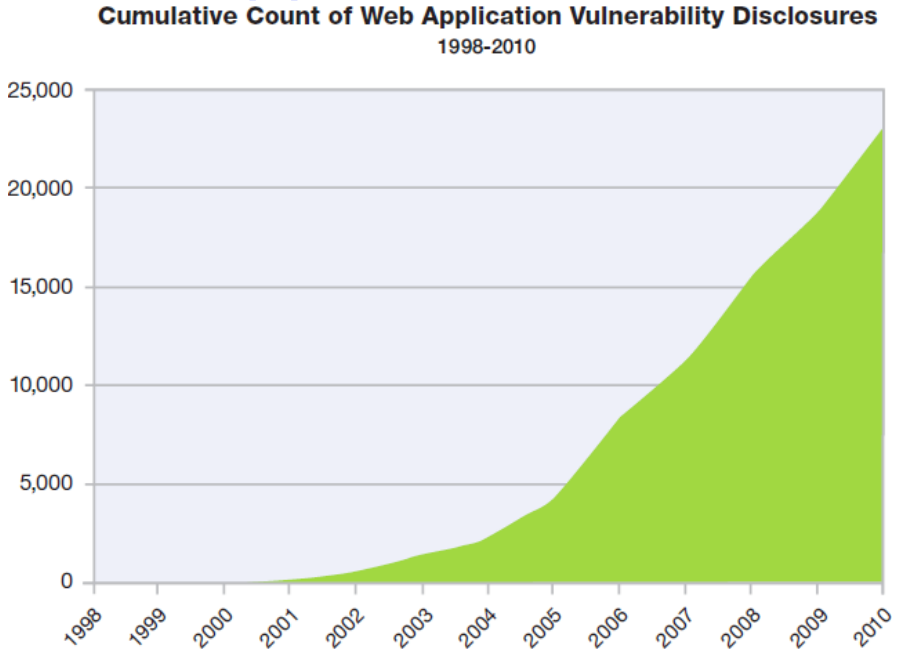
WHY?

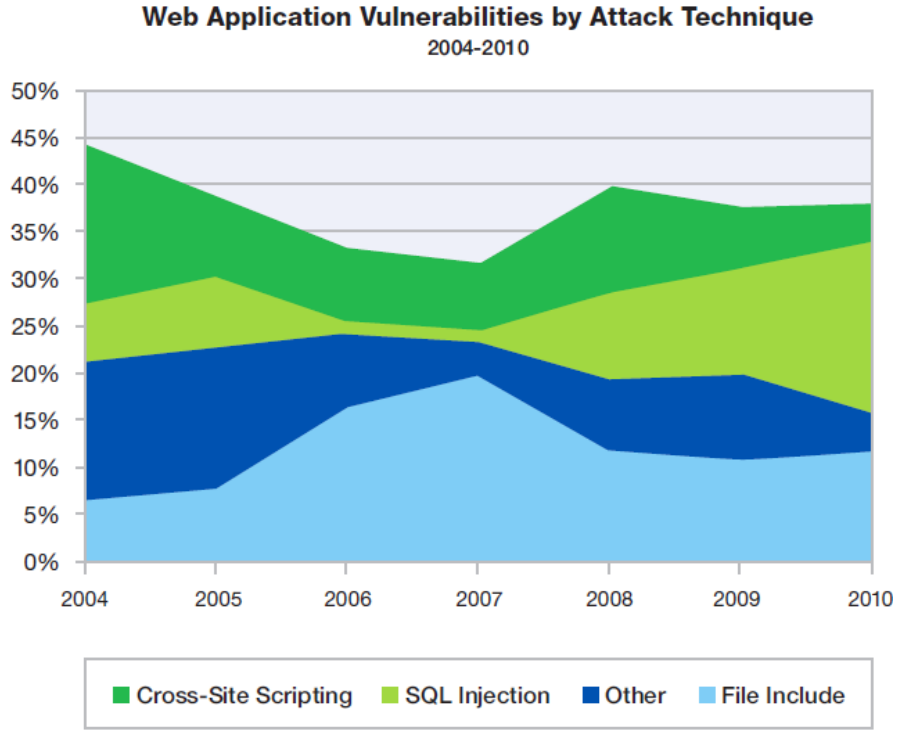
- Database servers contain your client's most valuable information
  - **Financial records**
  - **Customer information**
  - **Credit card and other account records**
  - **Personally identifiable information**
  - **Patient records**
- High volumes of structured data
- Easy to access

2012 Data Breach Report from Verizon Business RISK Team

http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

Web Application Vulnerabilities Continue to Rise

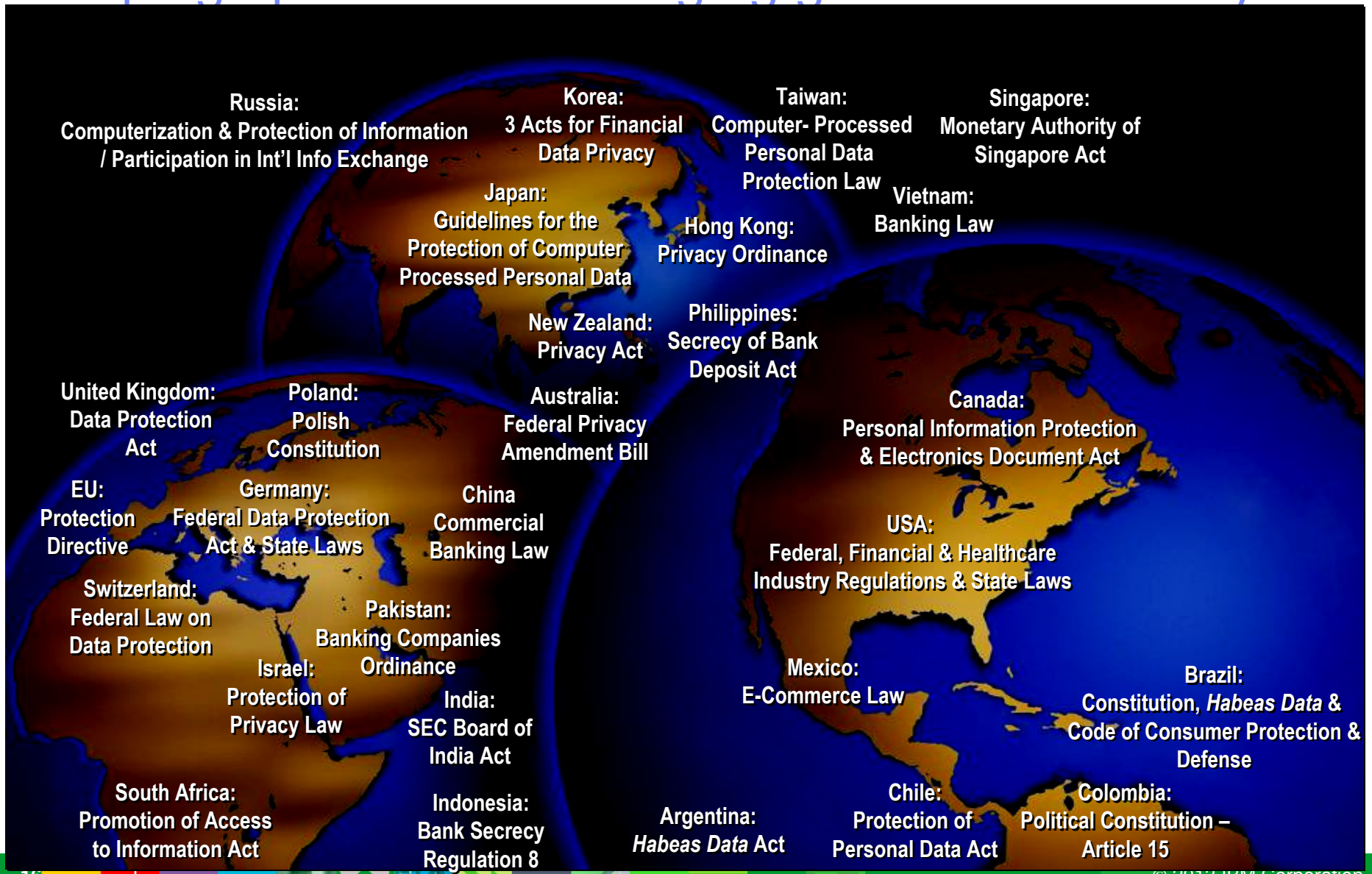




"The majority of web applications are custom … **the total number of web application vulnerabilities is likely much larger than the quantity of public reports** … Web application vulnerabilities may vastly exceed the quantity of other kinds of security issues on the Internet.

Source: IBM Security Solutions X-Force® 2010 Trend and Risk Report
www.ibm.com/security/xforce

Keeping up with ever-changing global and industry



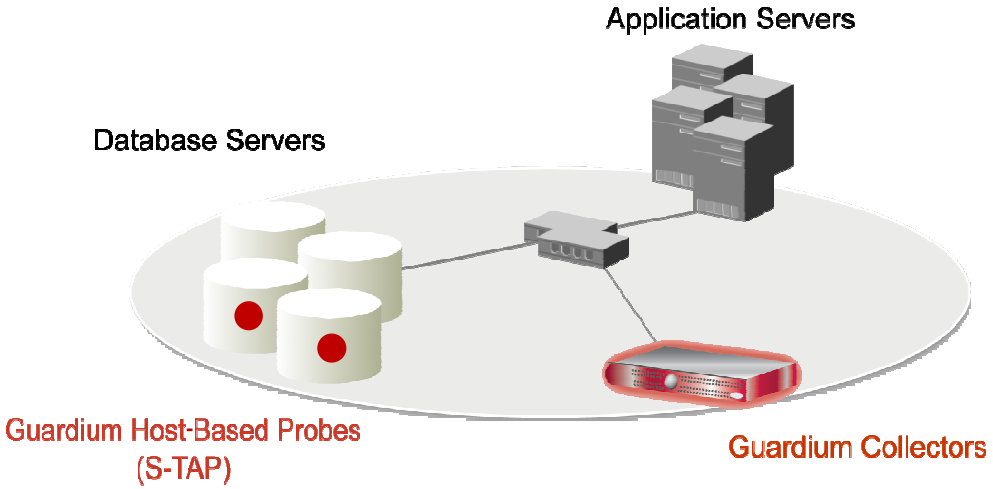
Key Business Drivers for Database Security & Compliance

1. Prevent data breaches
   - Prevent disclosure or leakages of sensitive data

2. Ensure the integrity of sensitive data
   - Prevent unauthorized changes to data, database structures, configuration files and logs

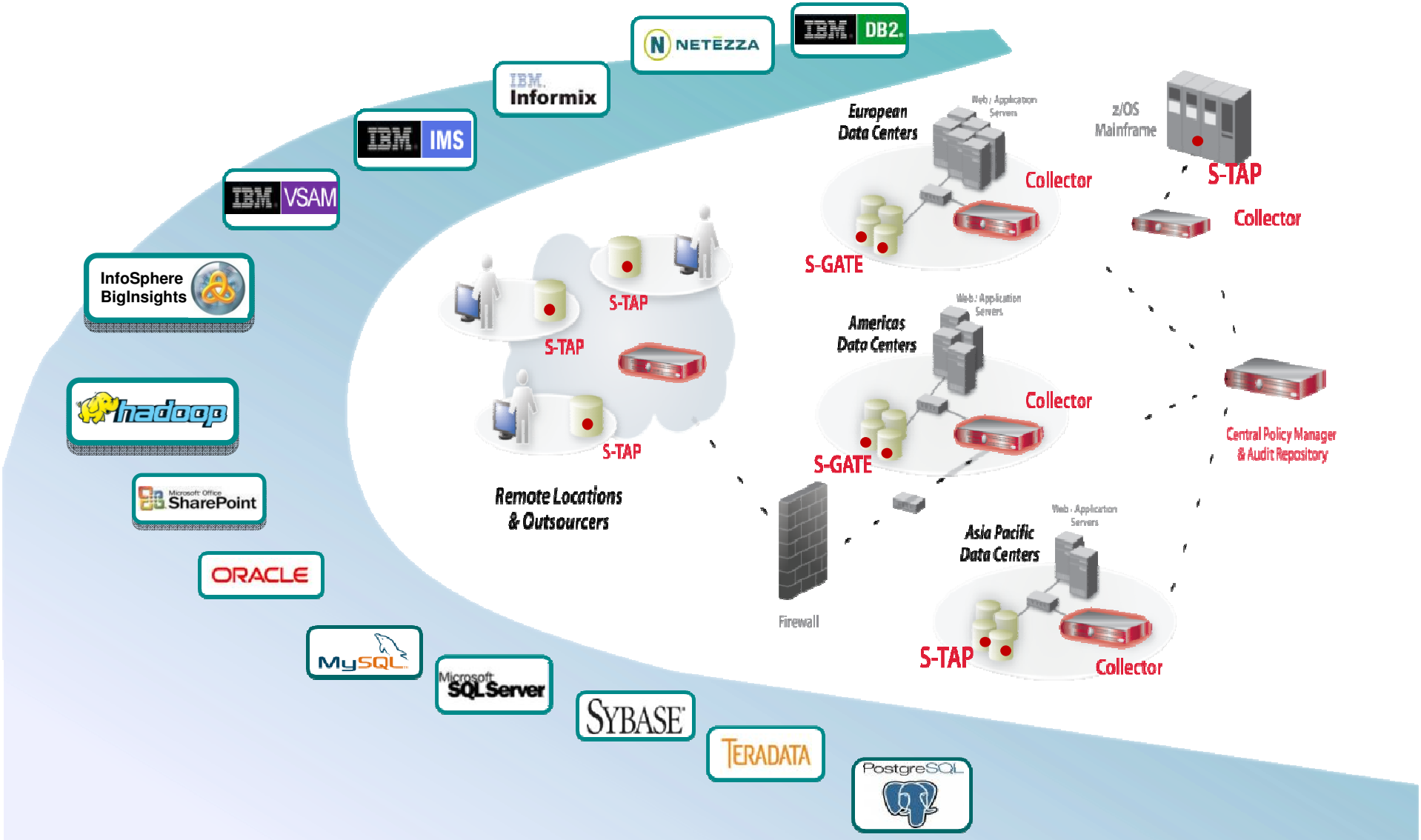
3. Reduce cost of compliance
   - Automate and centralize controls
     - Across diverse regulations, such as PCI DSS, data privacy regulations, HIPAA/HITECH etc.
     - Across heterogeneous environments such as databases, applications, data warehouses and Big Data platforms
   - Simplify the audit review processes

Non-Invasive, Real-Time Database Security & Monitoring

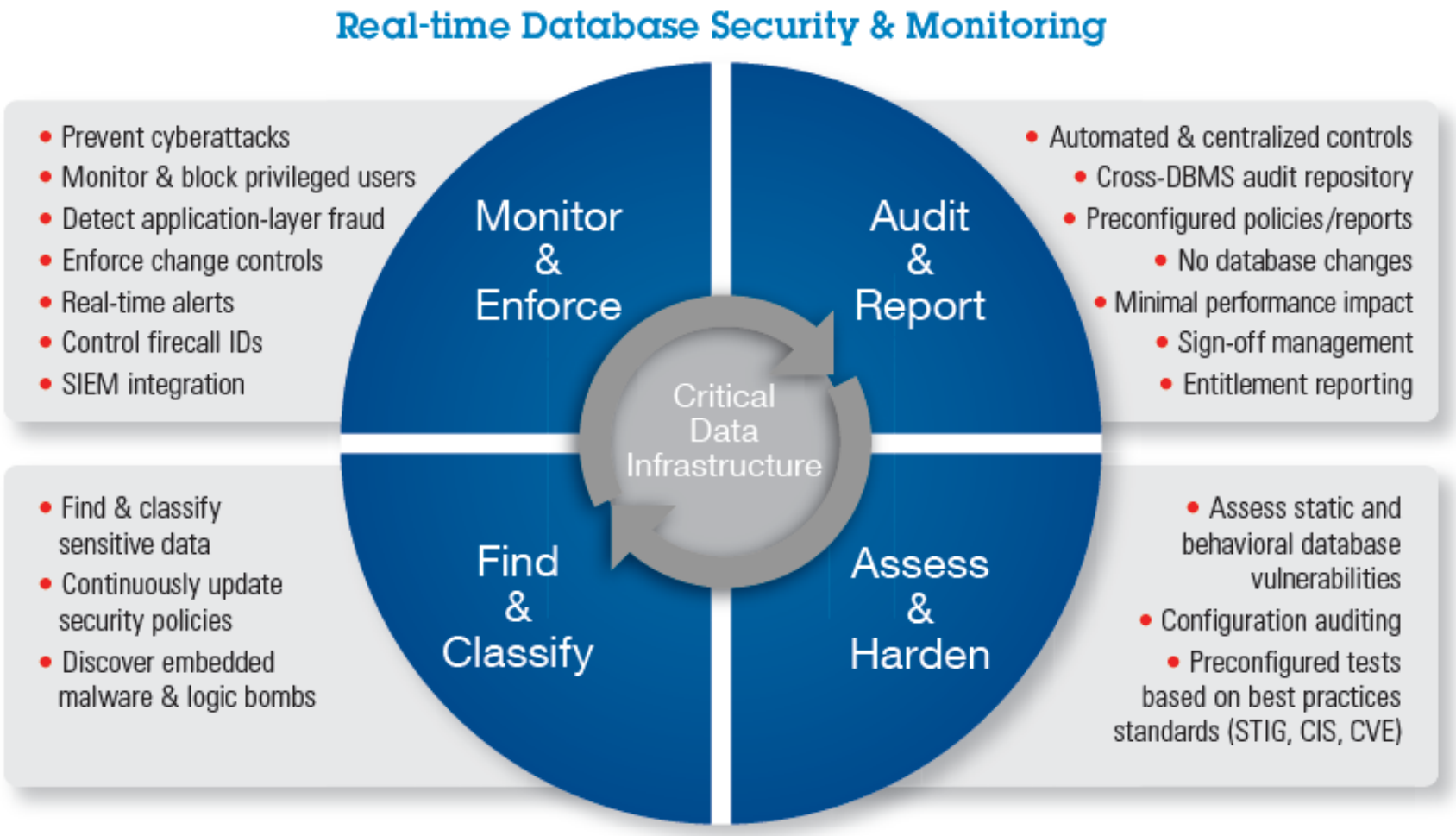


- Continuously monitors all database activities (including local access by superusers)
- Heterogeneous, cross-DBMS solution
- Does not rely on native DBMS logs
- Minimal performance impact (2-3%)
- No DBMS or application changes
- Supports Separation of Duties
- Activity logs can't be erased by attackers or DBAs
- Automated compliance reporting, sign-offs & escalations (SOX, PCI, NIST, etc.)
- Granular, real-time policies & auditing
  - *Who, what, when, where, how*

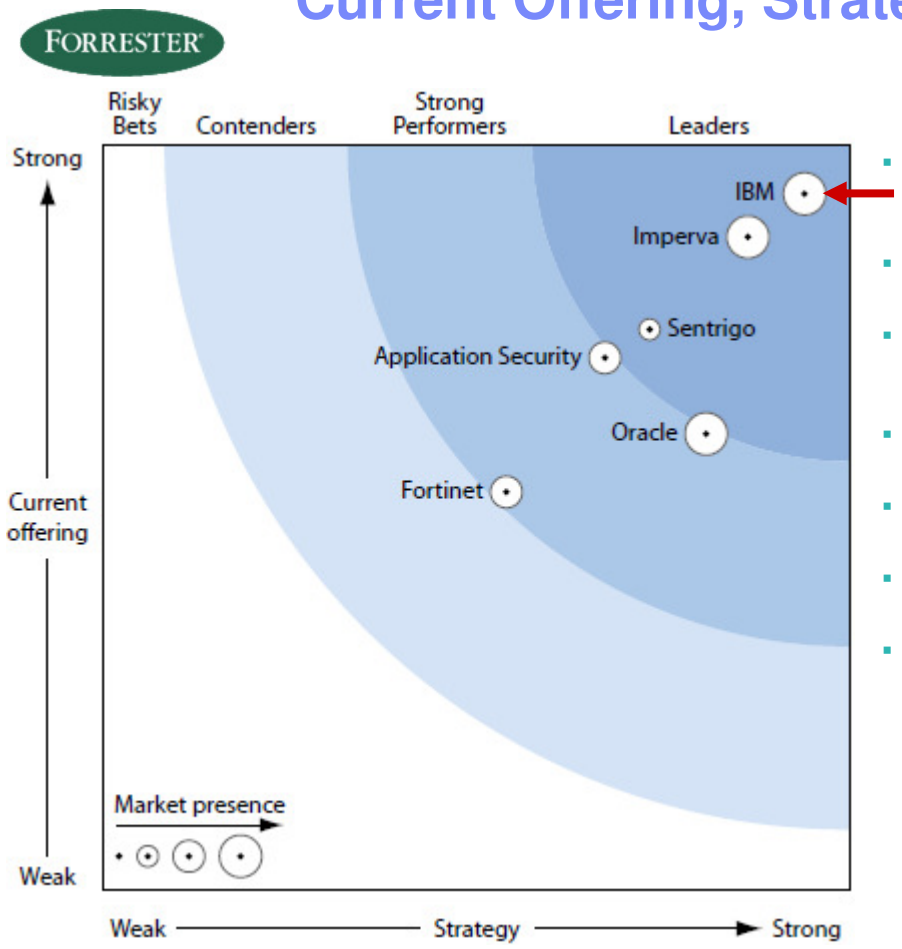
Heterogeneous Scalable Architecture



Addressing the Full Lifecycle of Database Security



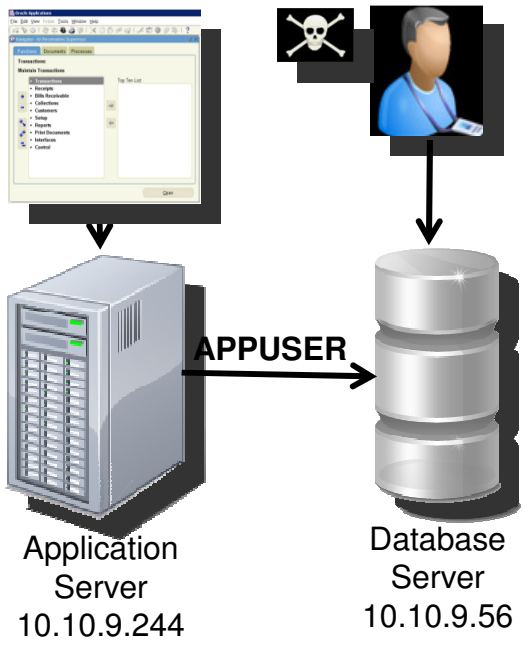
Highest Overall Score for Current Offering, Strategy, & Market Presence



- "***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.***"
- "***IBM continues to focus on innovation and extending the Guardium product to integrate with other IBM products.***"
- ***#1 score in all 3 Top Categories and all 17 subcategories along with perfect scores for Audit Policies; Auditing Repository; Corporate Strategy; Installed Base; Services; and International Presence.***
- "***Guardium offers support for almost any of the features that one might find in an auditing and real-time protection solution.***"
- "***Guardium offers strong support for database-access auditing, application auditing, policy management, auditing repository, and real-time protection.***"
- "***Guardium has been deployed across many large enterprises and hundreds of mission-critical databases.***"
- "***IBM offers comprehensive professional services to help customers with complex environments as well as those who need assistance implementing database security across their enterprise.***"

Source: "The Forrester Wave™: Database Auditing And Real-Time Protection, Q2 2011" (May 2011)

Granular Policies with Detective & Preventive Controls



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

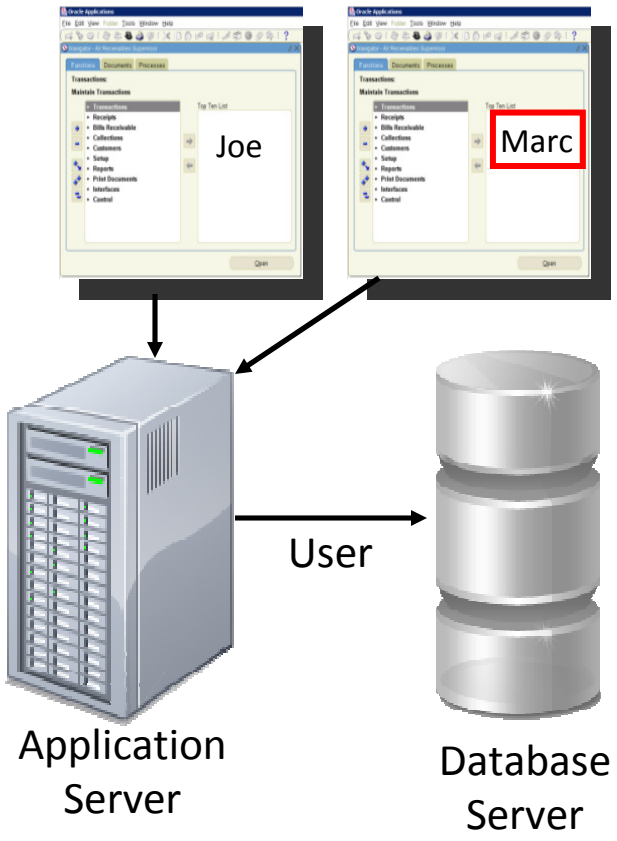
☒ Notification Type MAIL Mail User marc_gamache@guardium.com

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

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, WebLogic, ….)
  - Deterministic vs. time-based "best guess"
  - No changes to applications

Tracking Privileged Users Who "su"

Challenge: How do you track users who 'switch' accounts (perhaps to cover their tracks)?

- Native database logging/auditing & SIEM tools can't capture OS user information
- Other database monitoring solutions only provide OS shell account that was used

User activity

```
login as: joe
joe@192.168.30.152's password:
Last login: Tue Apr 14 15:17:12 2009 from 192.168.20.160
[joe@u2 ~]$ su - oracle
Password:
-bash-3.00$ sqlplus system

SQL*Plus: Release 10.2.0.1.0 - Production on Tue Apr 14 15:17:39 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> insert into AppUser.EmployeeTable values (1001,6,'Joe','Smith','Salary','Bonus',500000,1);

1 row created.

SQL>
```

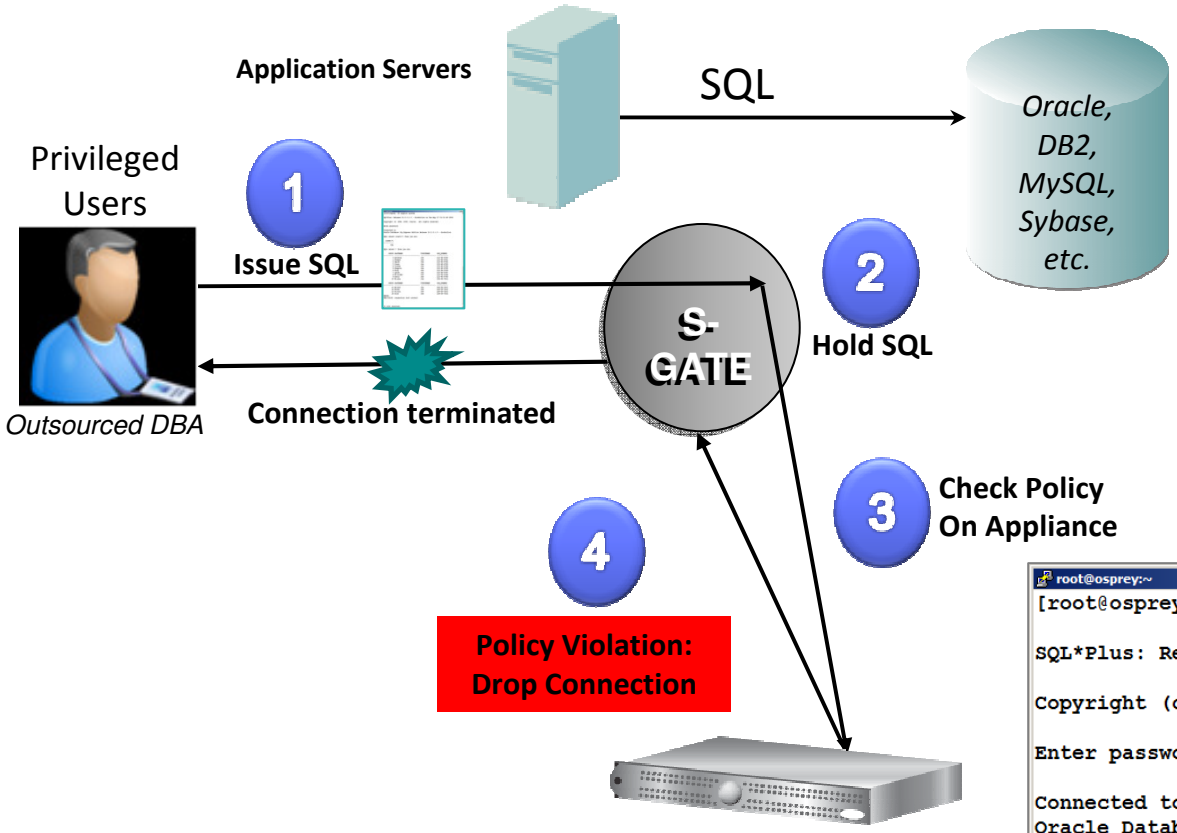
What Guardium Shows You

DB User Name	Sql
SYSTEM	insert into AppUser.EmployeeTable values (?,?,?,?,?,?,?,?)

DB User Name	ShellAcct	Sql
SYSTEM	ORACLE	insert into AppUser.EmployeeTable values (?,?,?,?,?,?,?,?)

DB User Name	ShellAcct	OSUser	Sql
SYSTEM	ORACLE	joe	insert into AppUser.EmployeeTable values (?,?,?,?,?,?,?,?)

Cross-DBMS, Data-Level Access Control (S-GATE)

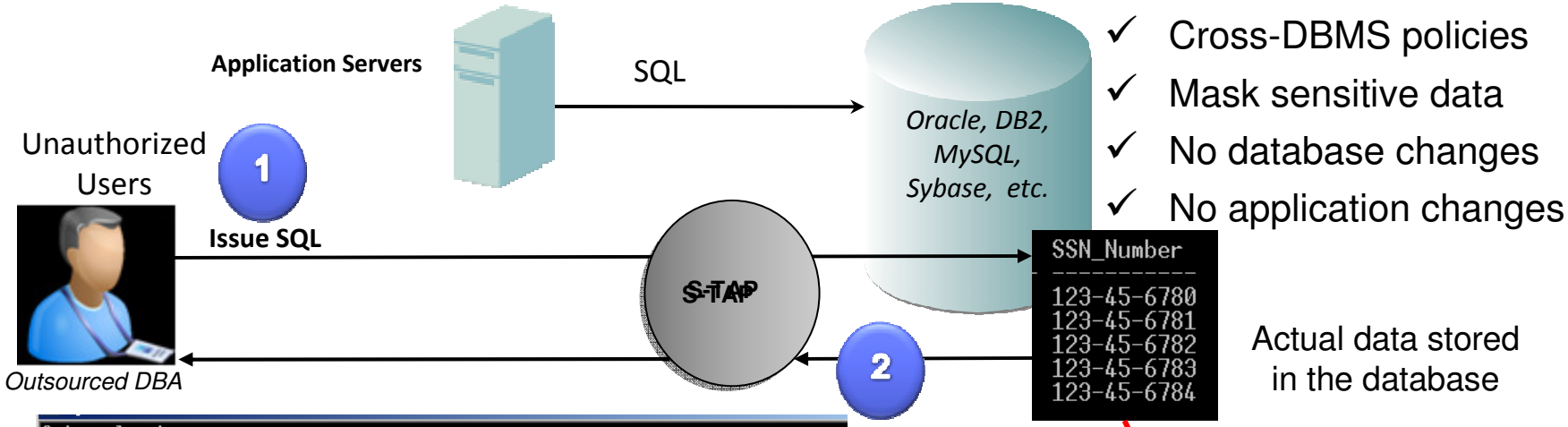


- ✓ Cross-DBMS policies
- ✓ Block privileged user actions
- ✓ No database changes
- ✓ No application changes
- ✓ Without risk of inline appliances that can interfere with application traffic

```
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

Unauthorized Users Masked when Sensitive Information Cross-DBMS, Data-Level Access Control (Redact)

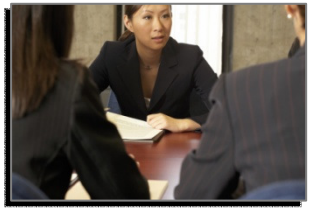


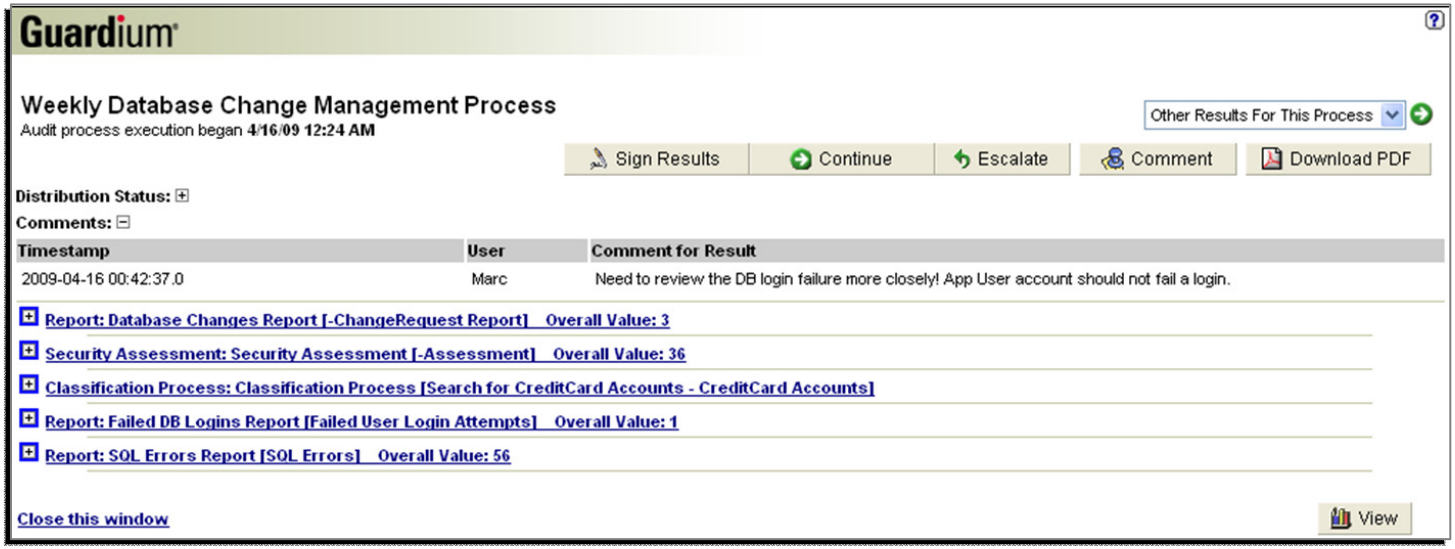
- ✓ Cross-DBMS policies
- ✓ Mask sensitive data
- ✓ No database changes
- ✓ No application changes

```
C:\>sqlcmd
1> select * from ssn where ssnid < 5
2> go
SSNID       LastName                  FirstName       SSN_Number
----------- ------------------------- --------------- -----------
          0 Anthony                   joe             *******-6780
          1 Thomas                    joe             *******-6781
          2 Smith                     Joe             *******-6782
          3 Jones                     Joe             *******-6783
          4 Craven                    Joe             *******-6784

(5 rows affected)
1> quit
```

User view of the data in the database

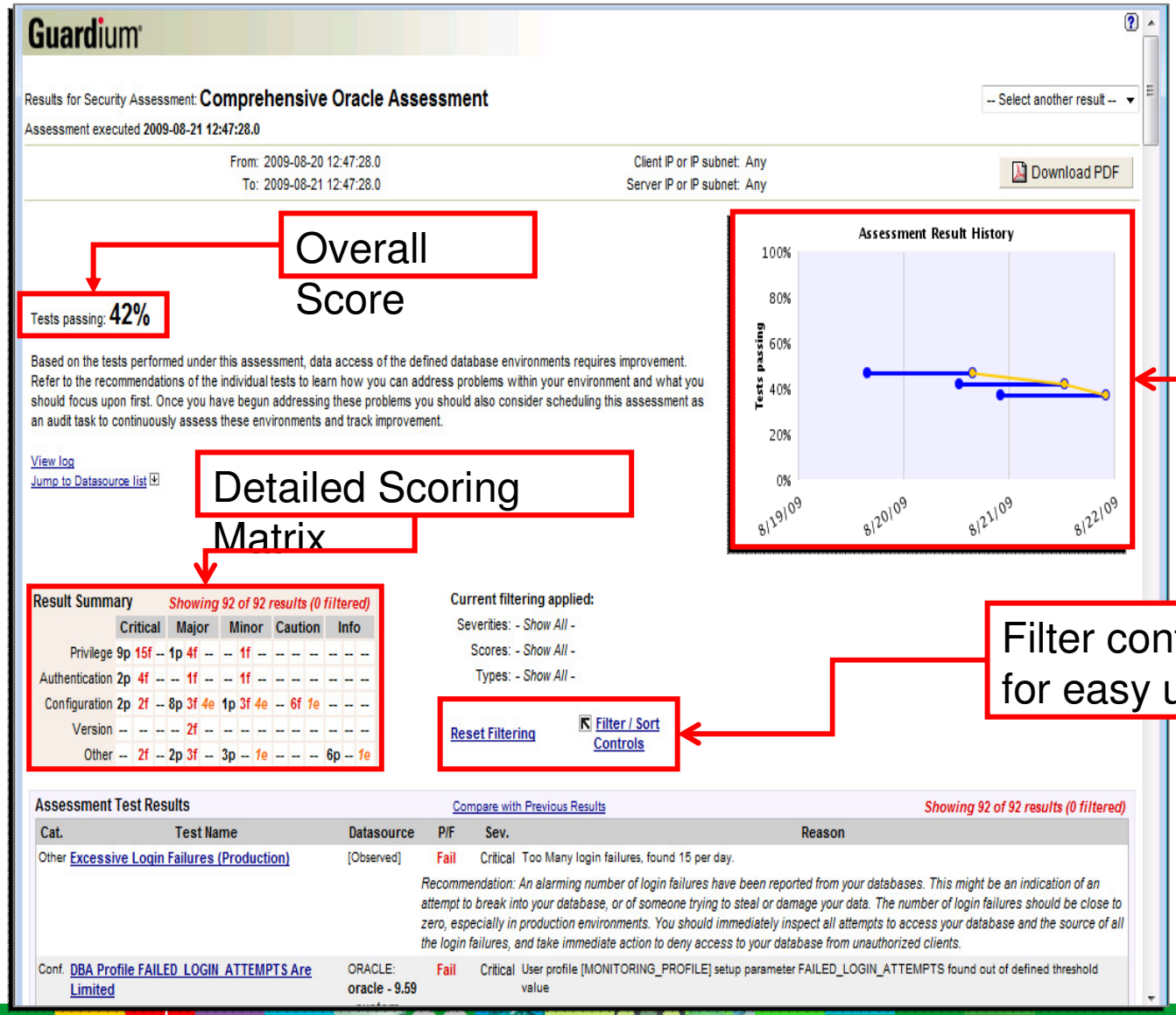
Automating Sign-offs & Escalations for Compliance





- 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

Vulnerability Assessments Using CIS, STIG Benchmarks



Validated by Industry Experts

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

"Most Powerful Compliance Regulations Tools ... Ever"

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

"Top of DBEP Class"

"Practically every feature you'll need [illegible]"

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

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

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

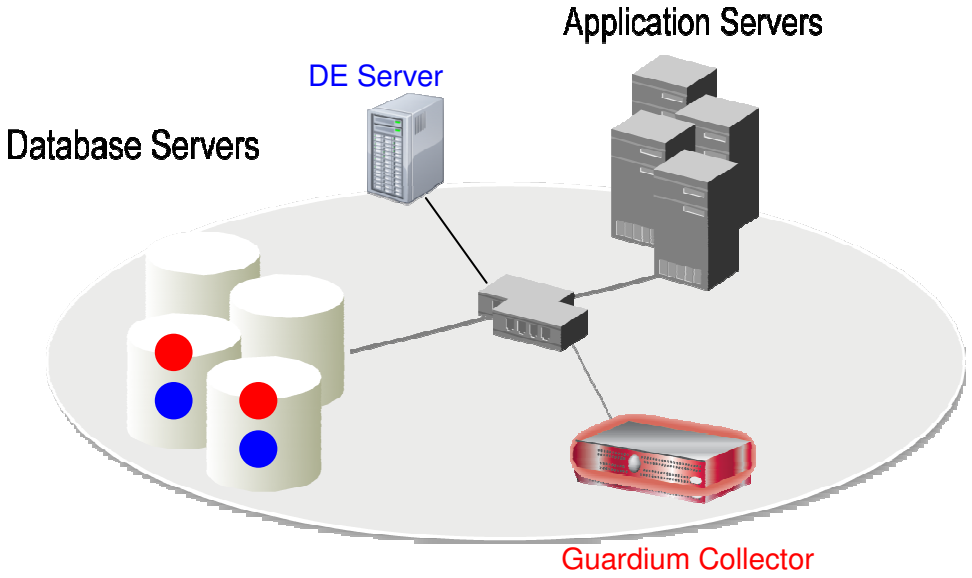
"Enterprise-class data security product that should be on every organization's radar."

InfoSphere Guardium Data Encryption

InfoSphere Guardium products

- **Guardium Data Encryption (DE) and Guardium Database Activity Monitor (DAM) are complimentary security products**

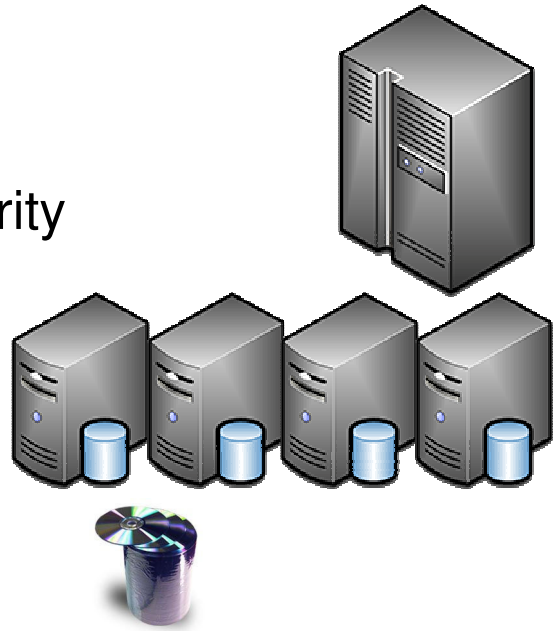
- **Guardium DAM Strength**
  - SQL Access Monitoring
  - SQL Intrusion Prevention
  - Auditing
  - Reporting



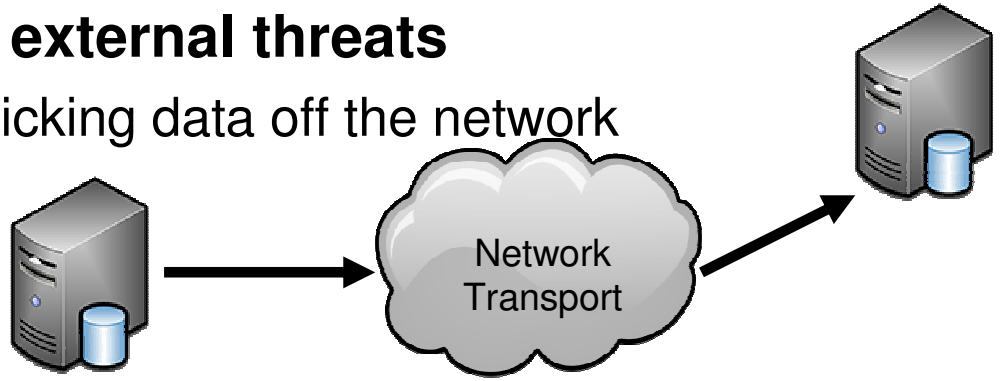
- **Guardium DE Strength**
  - Transparent Data Encryption
  - Key management
  - File Access Control

The Data Threats – Data at Rest & Data in Transit

- **Online – internal threats**
  - Attackers breaking through perimeter security
  - Privileged user abuse
  - Data replicates to many locations
- **Offline – theft and loss**
  - Backups typically written to portable media
  - Often stored offsite for long periods



- **Onwire – internal and external threats**
  - Hackers and sniffers picking data off the network



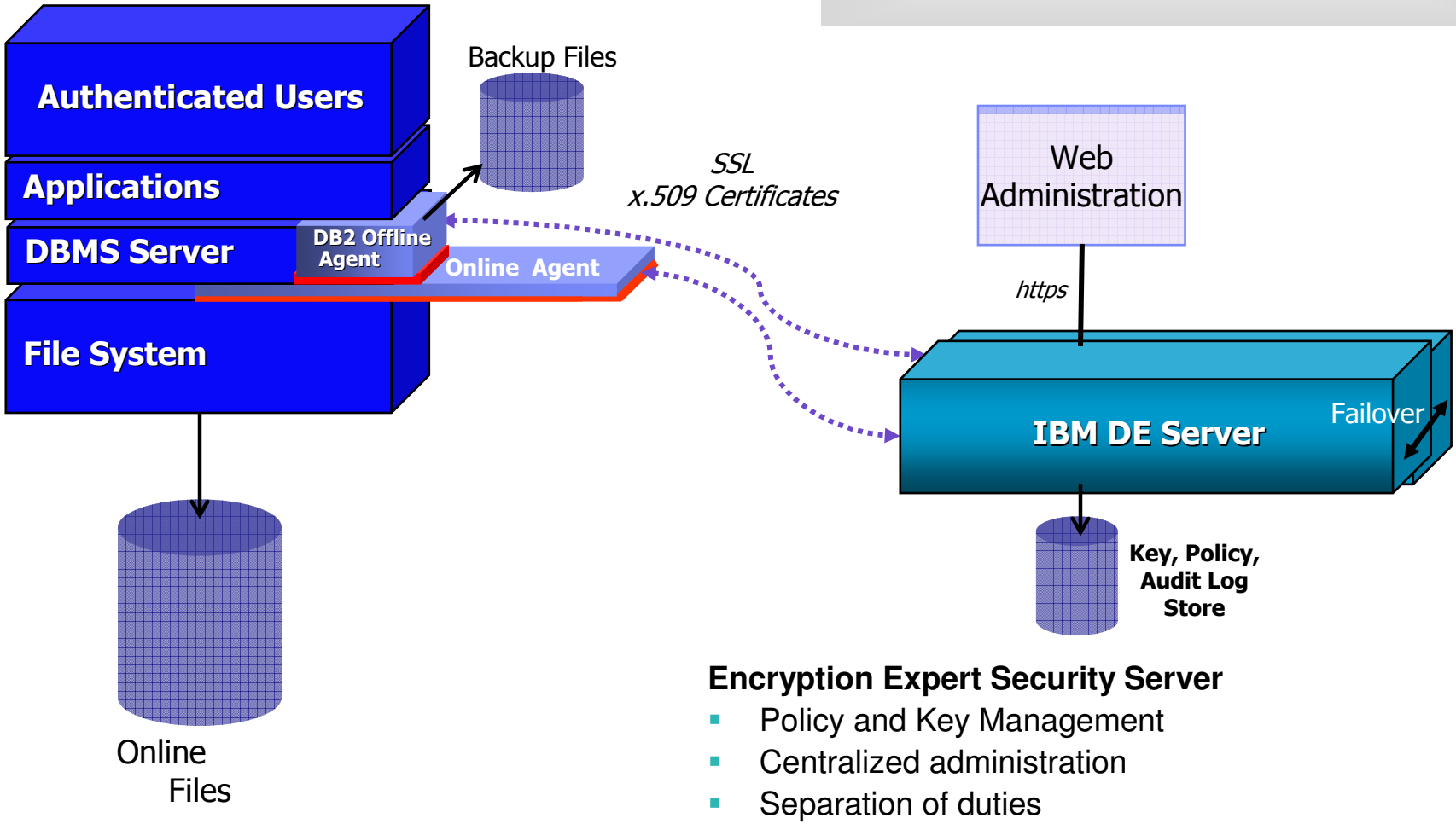
What is InfoSphere Guardium Data Encryption?

- **Data protection for your database environments**
  - High performance encryption, access control and auditing
  - Data privacy for both online and backup environments
  - Unified policy and key management for centralized administration across multiple data servers
- **Transparency to users, databases, applications, storage**
  - No coding or changes to existing IT infrastructure
  - Protect data in any storage environment
  - User access to data same as before
- **Centralized administration**
  - Policy and Key management
  - Audit logs
  - High Availability

Data Encryption Architecture

Components:

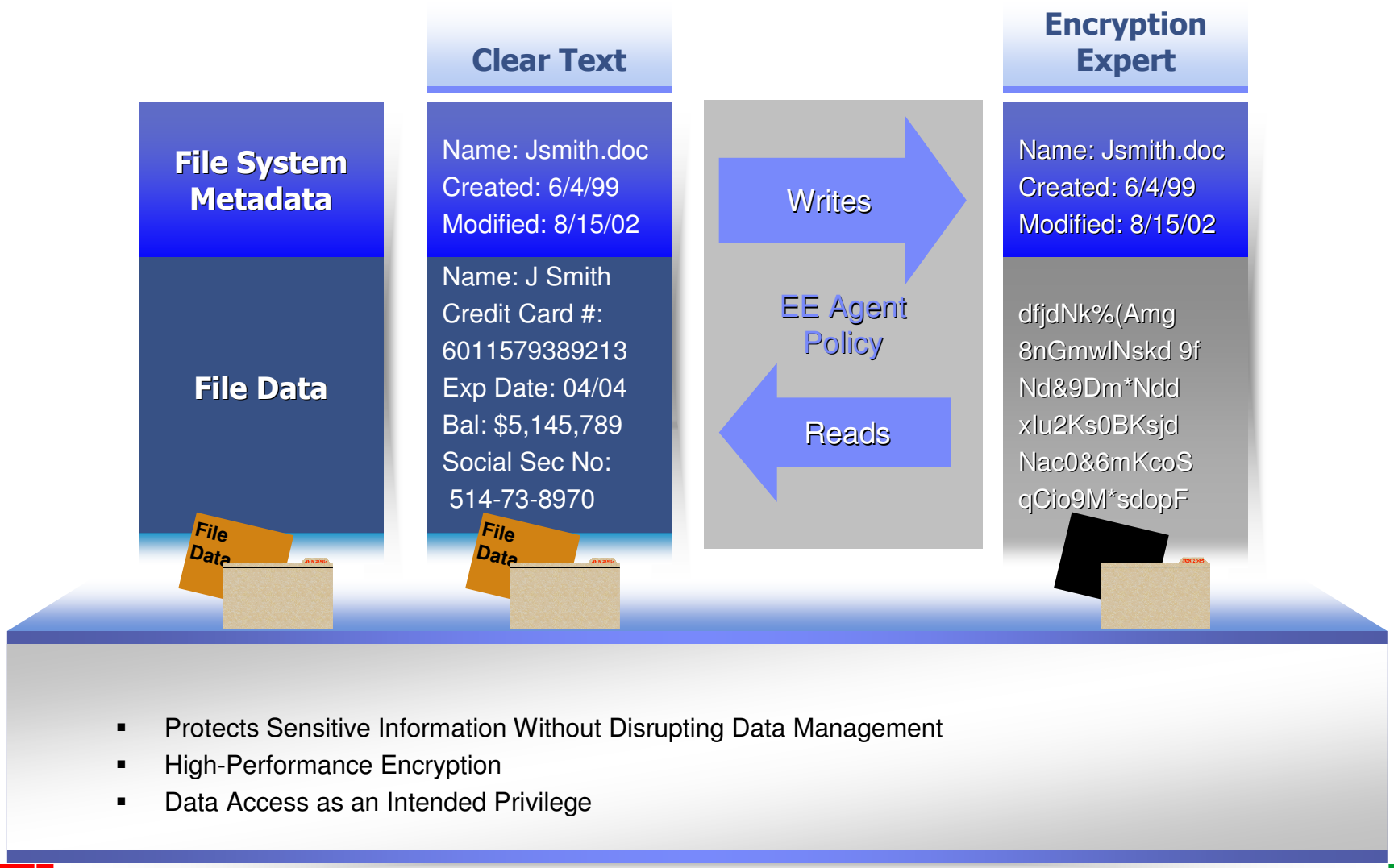
- DE Security Server
- DE Secure Offline Agent
- DE Secure File System Online Agent



Encryption Expert Security Server

- Policy and Key Management
- Centralized administration
- Separation of duties

File Management



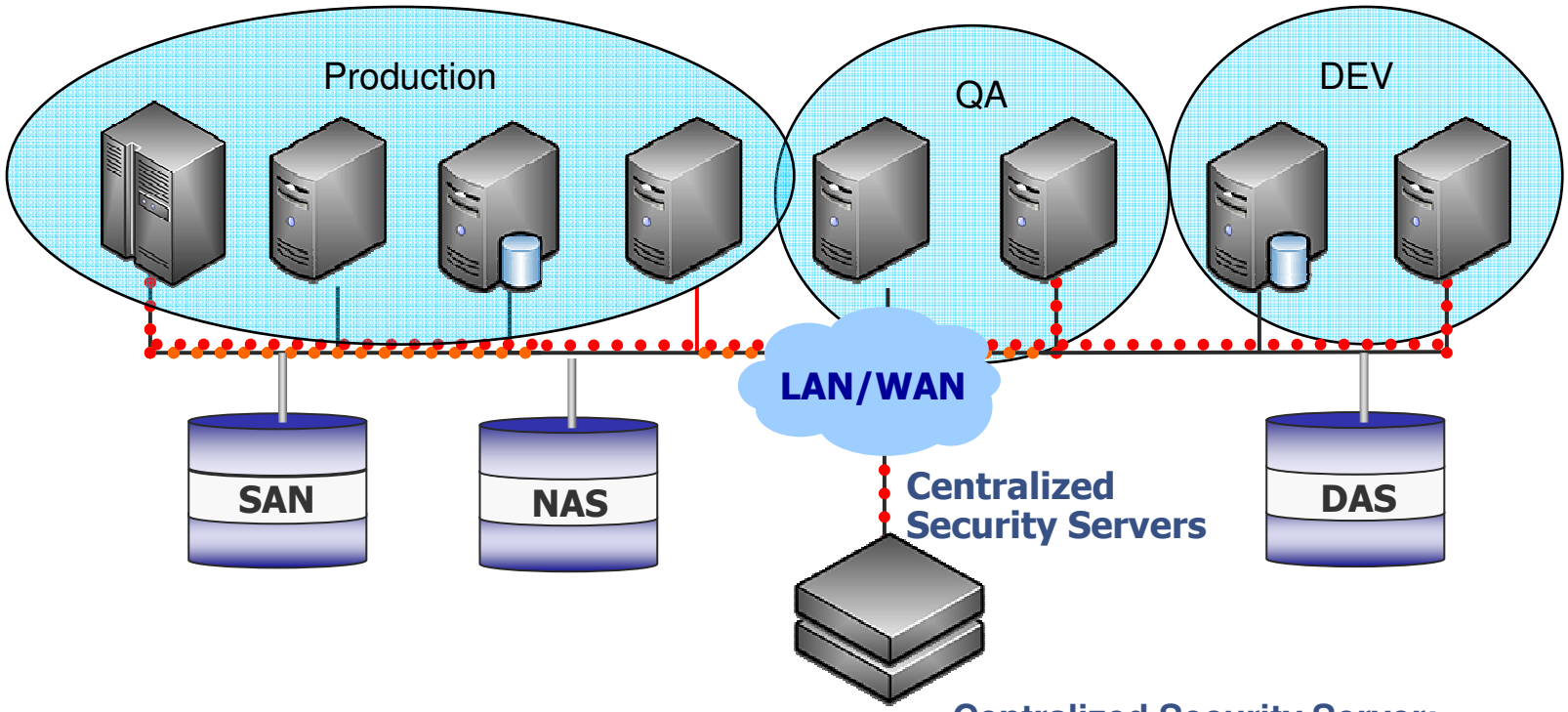
- Protects Sensitive Information Without Disrupting Data Management
- High-Performance Encryption
- Data Access as an Intended Privilege

Context-Aware Access Control

Who?	▼ Filters Users or Groups Who May Access Protected Data ▼ Filters the Applications Users May Invoke to Access Protected Data
What?	▼ Identifies the File System Operations Available to the User/ Application Combination
Where?	▼ Identifies Protected Data (e.g., File, Directory, Wildcard)
When?	▼ Verifies Authorized Time Window Available for Access by Window-Sensitive Tasks (e.g., Backup, Contract Employees)
How?	▼ Separates the Ability to ***Access*** Data From the Ability to ***View*** Data

Authentication **Authorization** **Audit**

Distributed Enforcement - Centralized Management



- **Centralized Security Server:**
  - **Multiple database instances**
  - **Online and Offline**
  - **Heterogeneous databases**

IBM InfoSphere Guardium Data Redaction

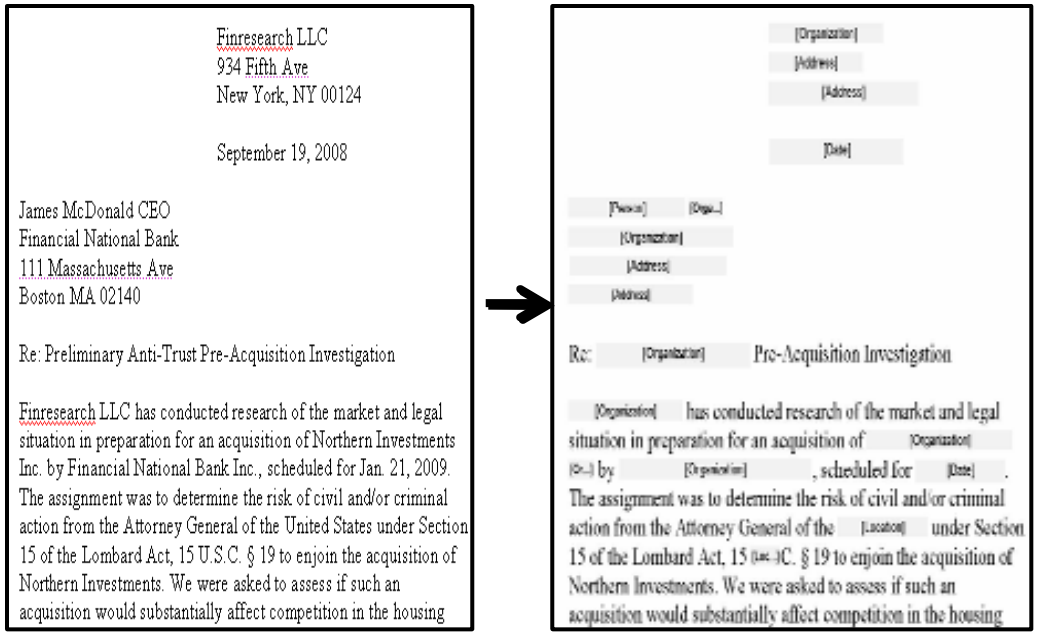
IBM Infosphere Guardium Data Redaction

Protect Sensitive Data Buried in Unstructured Documents and Forms

- **Protect sensitive *unstructured* data** in documents, forms and graphics
  - Finds and removes sensitive data and metadata from documents
  - Supports multiple file types: **PDF, TIFF, MS-Word, Txt**

- **Reduce the cost of compliance**
  - Balances automated extraction with human review via web-based console

- **Control unintentional data disclosure by user type**
  - Controls the data viewed by each user with policy rules
  - Integrate with enterprise LDAP security



Finresearch LLC
934 Fifth Ave
New York, NY 00124

September 19, 2008

James McDonald CEO
Financial National Bank
111 Massachusetts Ave
Boston MA 02140

Re: Preliminary Anti-Trust Pre-Acquisition Investigation

Finresearch LLC has conducted research of the market and legal situation in preparation for an acquisition of Northern Investments Inc. by Financial National Bank Inc., scheduled for Jan. 21, 2009. The assignment was to determine the risk of civil and/or criminal action from the Attorney General of the United States under Section 15 of the Lombard Act, 15 U.S.C. § 19 to enjoin the acquisition of Northern Investments. We were asked to assess if such an acquisition would substantially affect competition in the housing

[Organization]
[Address]
[Address]

[Date]

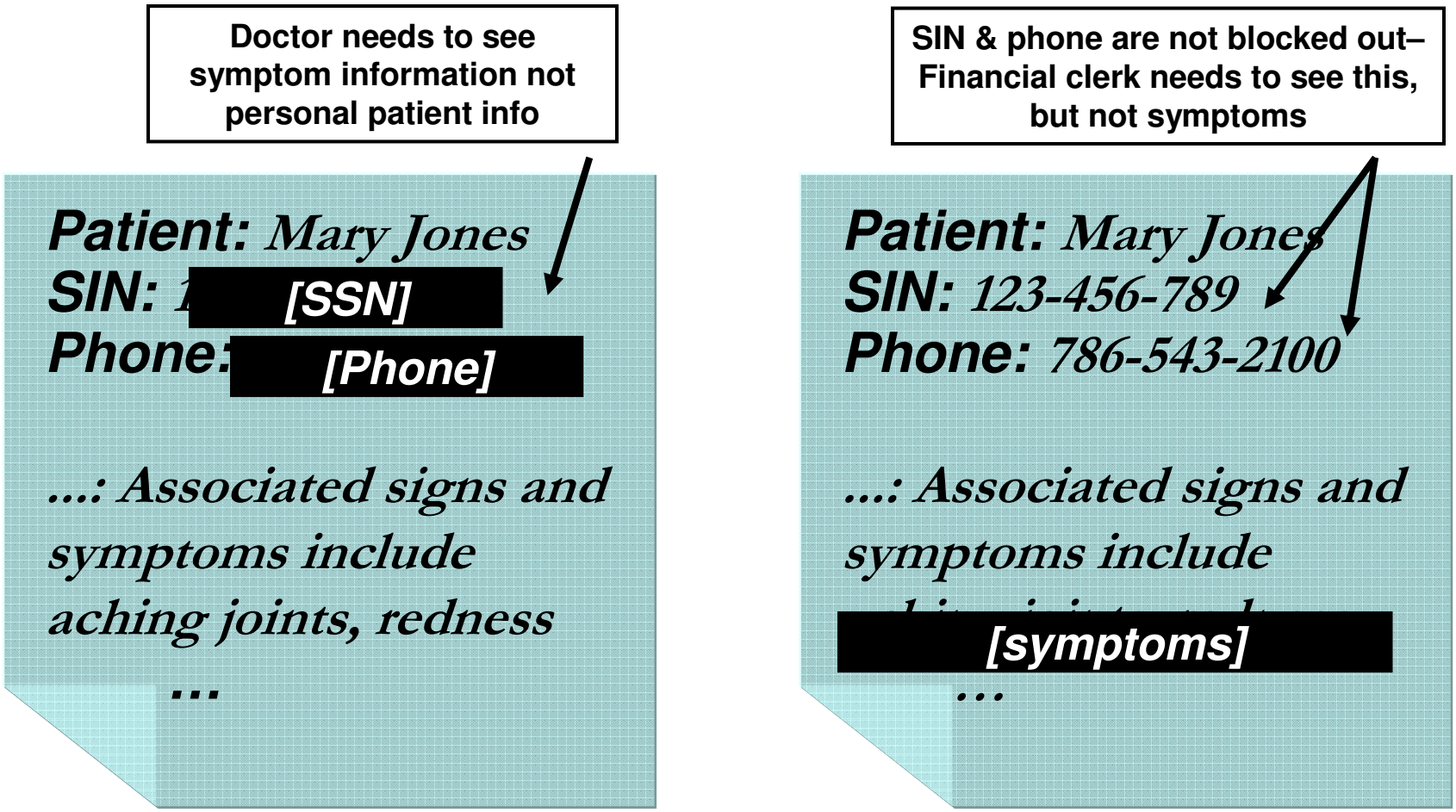
[Organization]
[Address]
[Address]

Re: [Organization] Pre-Acquisition Investigation

[Organization] has conducted research of the market and legal situation in preparation for an acquisition of [Organization] by [Organization], scheduled for [Date]. The assignment was to determine the risk of civil and/or criminal action from the Attorney General of the [Location] under Section 15 of the Lombard Act, 15 U.S.C. § 19 to enjoin the acquisition of Northern Investments. We were asked to assess if such an acquisition would substantially affect competition in the housing

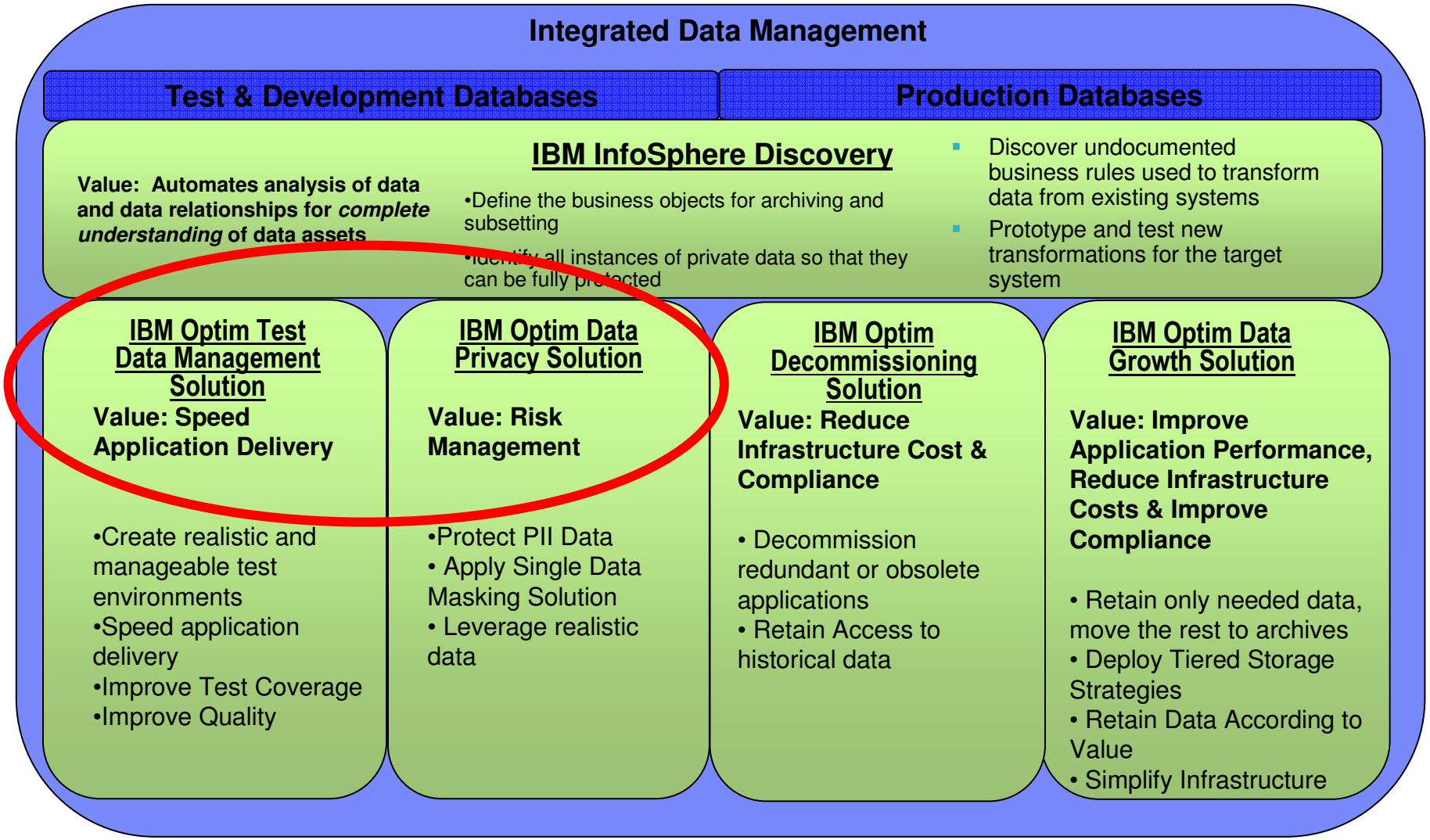
Guardium Data Redaction

Role-based security for compliance requirements

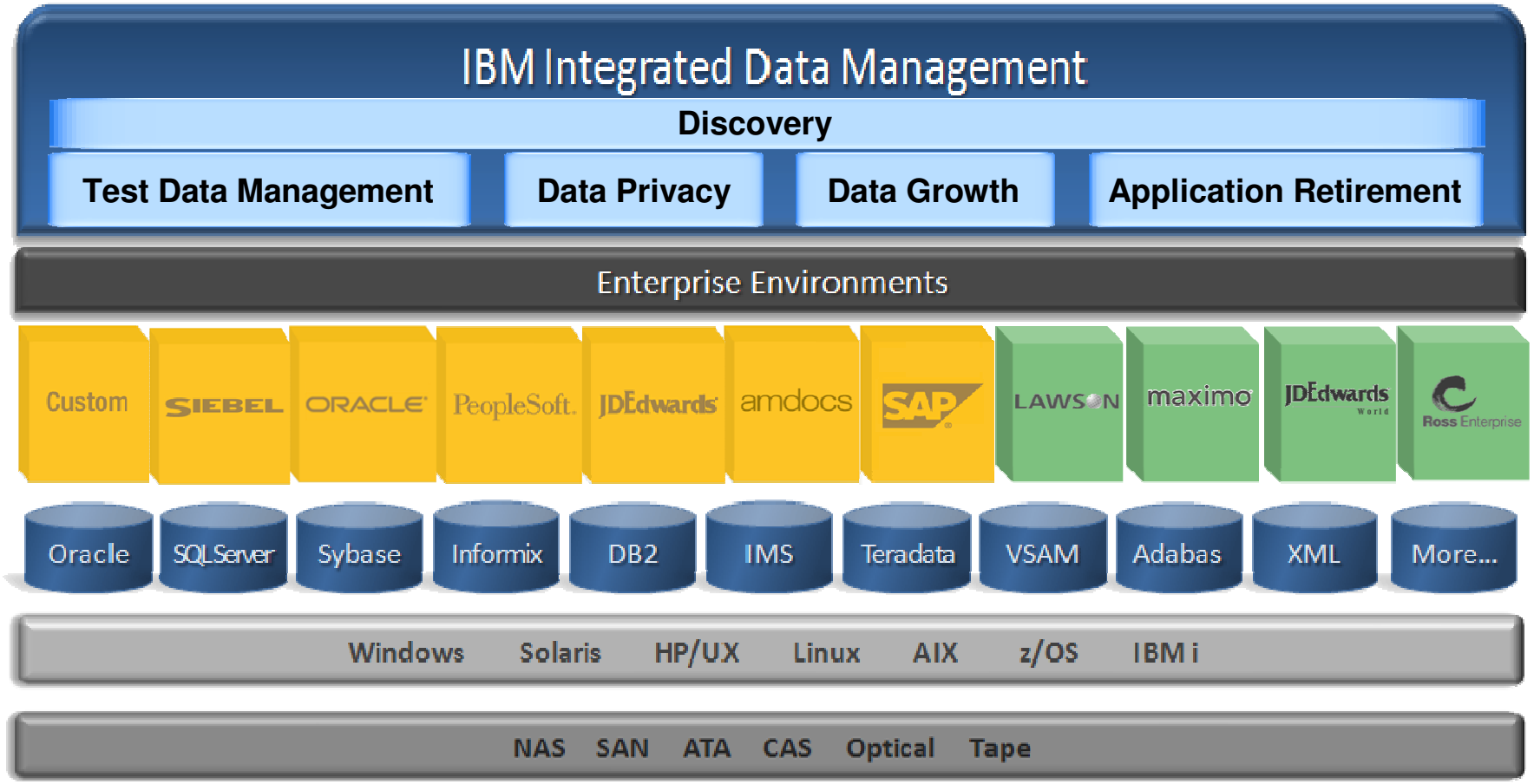


IBM InfoSphere Optim Data Privacy

Optim is a Platform for Integrated Data Management



Optim Enterprise Architecture



An integrated, modular environment to manage enterprise application data and optimize data-driven applications from requirements to retirement across heterogeneous environments.

The Easiest Way to Expose Private Data … Internally with the Test Environment

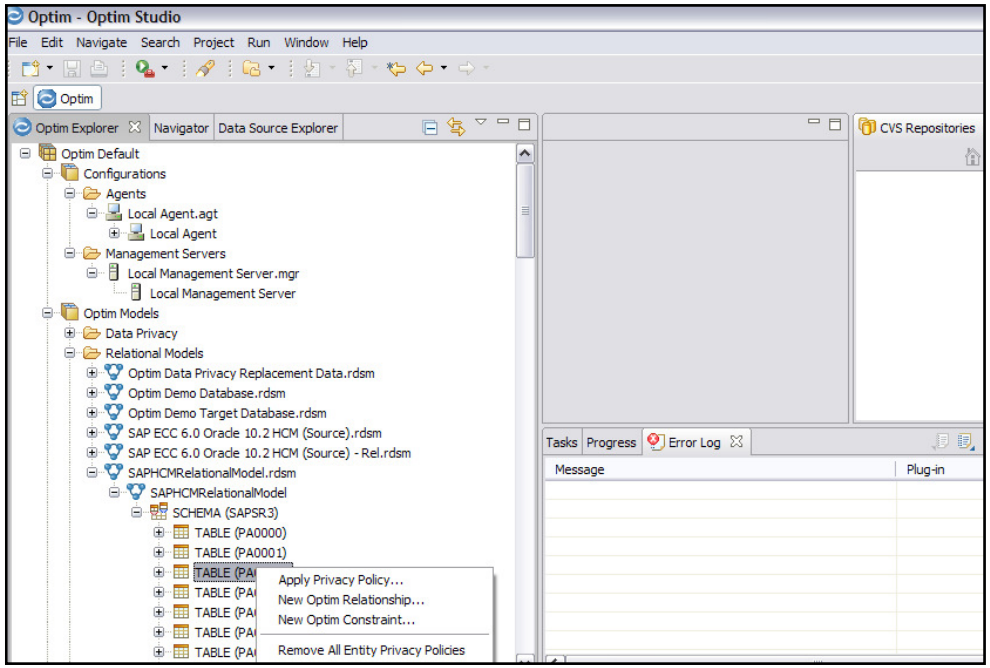
- 70% of data breaches occur internally (Gartner)
- Test environments use personally identifiable data
- Standard NDAs may not deter a disgruntled employee
- What about test data stored on laptops?
- What about test data sent to outsourced/overseas consultants?
- PCI DSS Reg. 6.3.4 states, "Production data (real credit card numbers) cannot be used for testing or development"

*** The Solution is Data De-Identification ***

IBM InfoSphere Optim Data Masking Solution

De-identify sensitive information with realistic *but fictional* data for testing & development purposes

Data Privacy



Optim Data Masking supports data on distributed platforms (LUW) and z/OS.
Out-of-the-box support for packaged applications available for ERP/CRM solutions:

Requirements

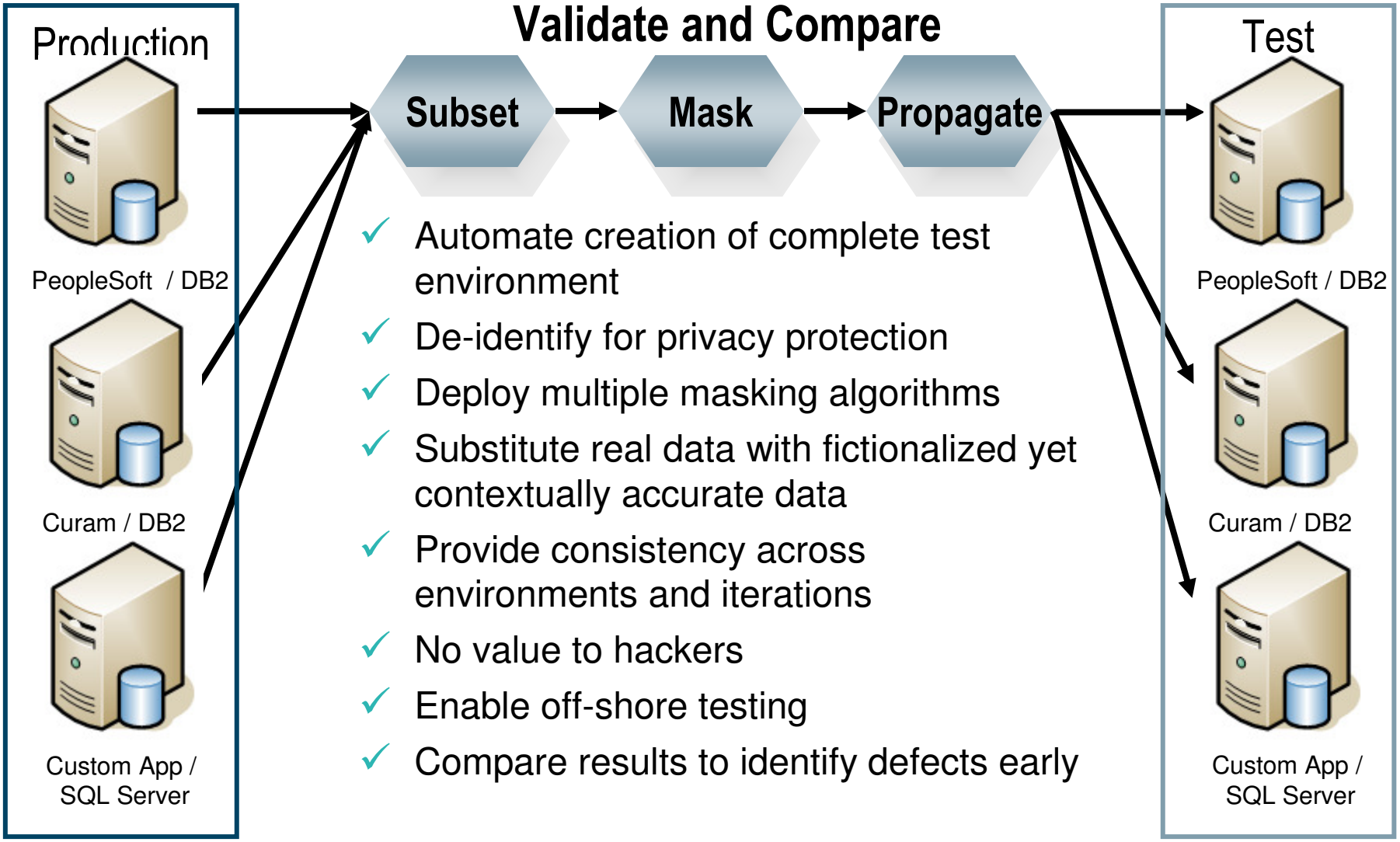
- Protect confidential data in test, training & development systems
- Consolidate and mask data from multiple interrelated applications to create a “production-like” test environment
- Apply a range of predefined or custom data masking techniques

Benefits

- Prevent data misuse/ breaches & associated fines
- Speed testing to accelerate time to market
- Reduce manual effort and manage costs

ORACLE e-businesssuite | PeopleSoft | SIEBEL | JDEdwards Enterprise Software | SAP | amdocs | Other

Optim Data Privacy and Test Data Management



- ✓ Automate creation of complete test environment
- ✓ De-identify for privacy protection
- ✓ Deploy multiple masking algorithms
- ✓ Substitute real data with fictionalized yet contextually accurate data
- ✓ Provide consistency across environments and iterations
- ✓ No value to hackers
- ✓ Enable off-shore testing
- ✓ Compare results to identify defects early

A Comprehensive Solution for Data Privacy is Needed

A comprehensive set of data masking techniques to transform or de-identify data, including:

String literal values
Character substrings
Random or sequential numbers
Arithmetic expressions
Concatenated expressions
Date aging
Lookup values
Intelligence

Example 1

Client Case Information

Patient No.	123456	**SIN**	987-654-321		
Name	Erica Schafer				
Address	12 Murray Court				
City	Vancouver	**Prov**	BC	**Zip**	V1V1V1

Data is masked with contextually correct data to preserve integrity of test data

Example 2

Personal Info Table

PersNbr	FirstName	LastName
10000	Jeanne	Renoir
10001	Claude	Monet
10002	**Pablo**	**Picasso**

Referential integrity is maintained with key propagation

Event Table

PersNbr	FstNEvtOwn	LstNEvtOwn
10002	**Pablo**	**Picasso**
10002	**Pablo**	**Picasso**

Large Regional Bank

Monitors database activity to support compliance regulations

The need:

Prevent users from inappropriately accessing or jeopardizing the integrity of enterprise data. Protect financial and transactional data including: payment card primary account numbers (PAN data), automatic cleansing house (ACH) transaction data and human resources (HR) data. Comply with Sarbanes-Oxley, Payment Card Industry Data Security Standard (PCI-DSS) and other financial privacy and audit regulations.

The solution:

Implemented IBM InfoSphere Guardium Database Activity Monitor to monitor end-user and privileged user activity across the IBM DB2, Oracle Database, MS SQL Server, and MySQL databases in the AIX, Solaris, Windows and Linux environments.

The benefits:

- Effectively monitors database activity for over 800 banking branches and supports compliance with privacy and audit regulations
- Helps prevent fraud and delivers return on investment with capabilities to identify suspicious database activities
- Supports data governance by preventing unauthorized changes to critical database values and structures

"Monitoring database activity with IBM Guardium is helping us support compliance with our privacy and audit requirements without impacting database performance."

— Source: Senior DBA, Large Regional Bank

Solution components:

- IBM InfoSphere Guardium Database Activity Monitor

CSFi

The need:

CSFi needed to satisfy PCI DSS. This meant ensuring that no device or system retains cardholder data while trying to grow in new overseas markets to beat the competition and increase revenues.

The solution:

CSFi used InfoSphere Guardium Data Encryption to satisfy PCI DSS rather than using column level encryption which can slow performance and is difficult to implement.

The benefits:

- Ensure compliance with Payment Card Industry Data Security Standard (PCI DSS)
- Allow IT staff to focus on value recreation and not tedious manual tasks
- Achieve all security and privacy requirements while maximizing system throughput
- Meet SLAs for processing transactions in just a few milliseconds

Solution components:

- IBM InfoSphere Guardium Data Encryption
- IBM Informix Dynamic Server

Arek Oy

Deploys a pension earnings and accrual system in 30 months

The need:

Pension laws (TyEL) in Finland changed radically in 2007. In response, Arek Oy had to develop and deliver a tested and reliable Pension Earnings and Accrual System within 30 months. Arek Oy had to protect confidential employee salary and pension information in multiple non-production (development and testing) environments. Failure to satisfy requirements would result in loss of customer good will and future business opportunities.

The solution:

Using IBM InfoSphere Optim subsetting capabilities rather than cloning large production databases made it possible for Arek Oy staff to create robust, realistic test databases that supported faster iterative testing cycles. In addition, InfoSphere Optim offered proven capabilities for performing complex data masking routines, while preserving the integrity of the pension data for development and testing purposes.

The benefits:

- Improved development and testing efficiencies, enabling Arek Oy to promote faster deployment of new pension application functionality and enhancements
- Protected confidential data to strengthen public confidence and support TyEL compliance requirements

"We see Optim as an integral part of our development solution set. Optim's data masking capabilities help ensure that we can protect privacy in our development and testing environments."

— Katri Savolainen, Project Manager, Arek Oy

Solution components:

- IBM InfoSphere Optim Data Masking Solution
- IBM InfoSphere Optim Test Data Management Solution

arek

Arek Oy Case Study

Questions