SmarterAnalytics

**TEO Wan Ping**

*teowping@sg.ibm.com*

*Information Governance, ASEAN*

# Security and Compliance

*Protecting data privacy and ensuring data security & compliance*

# 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

*Insiders*
*(DBAs, developers, outsourcers, etc.)*

*Outsourcing*

*Stolen Application Credentials (Zeus, etc.)*

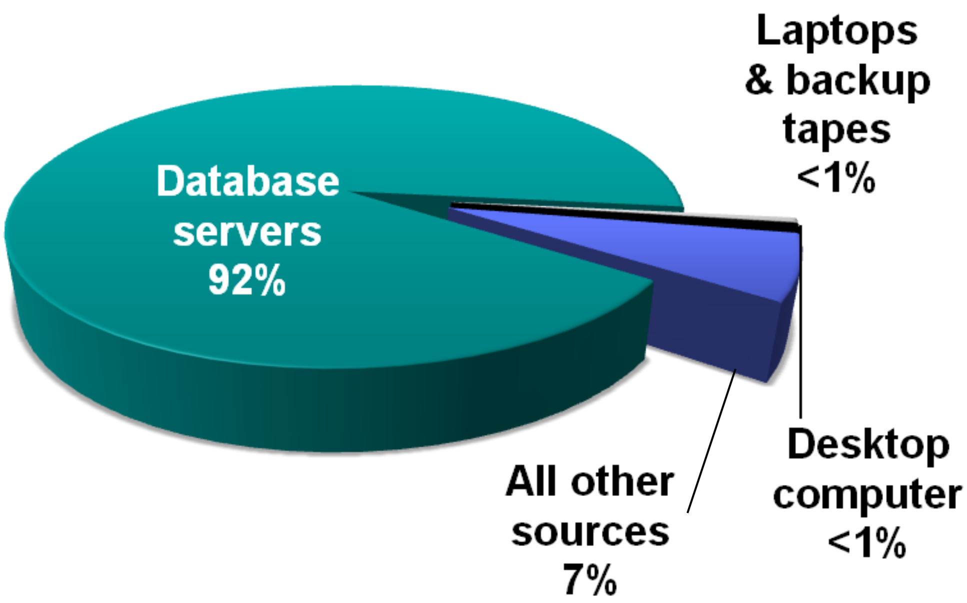
*Web-Facing Apps*

*Legacy App Integration/SOA*

*Employee Self-Service, Partners & Suppliers*

# Database Servers Are The Primary Source of Breached Data

% of Records Breached (2010)



*…up from 75% in 2009*

## Why Traditional DLP Isn't Sufficient

> "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."**
>
> **- 2009 Data Breach Investigations Report**

Source: http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf    Note: multi-vector breaches counted in multiple categories

# Key Business Drivers for Database Security & Compliance

1. **Prevent data breaches**

   Mitigate external & internal threats

2. **Assure data governance**

   Prevent unauthorized changes to sensitive data by privileged users

3. **Reduce cost of compliance**

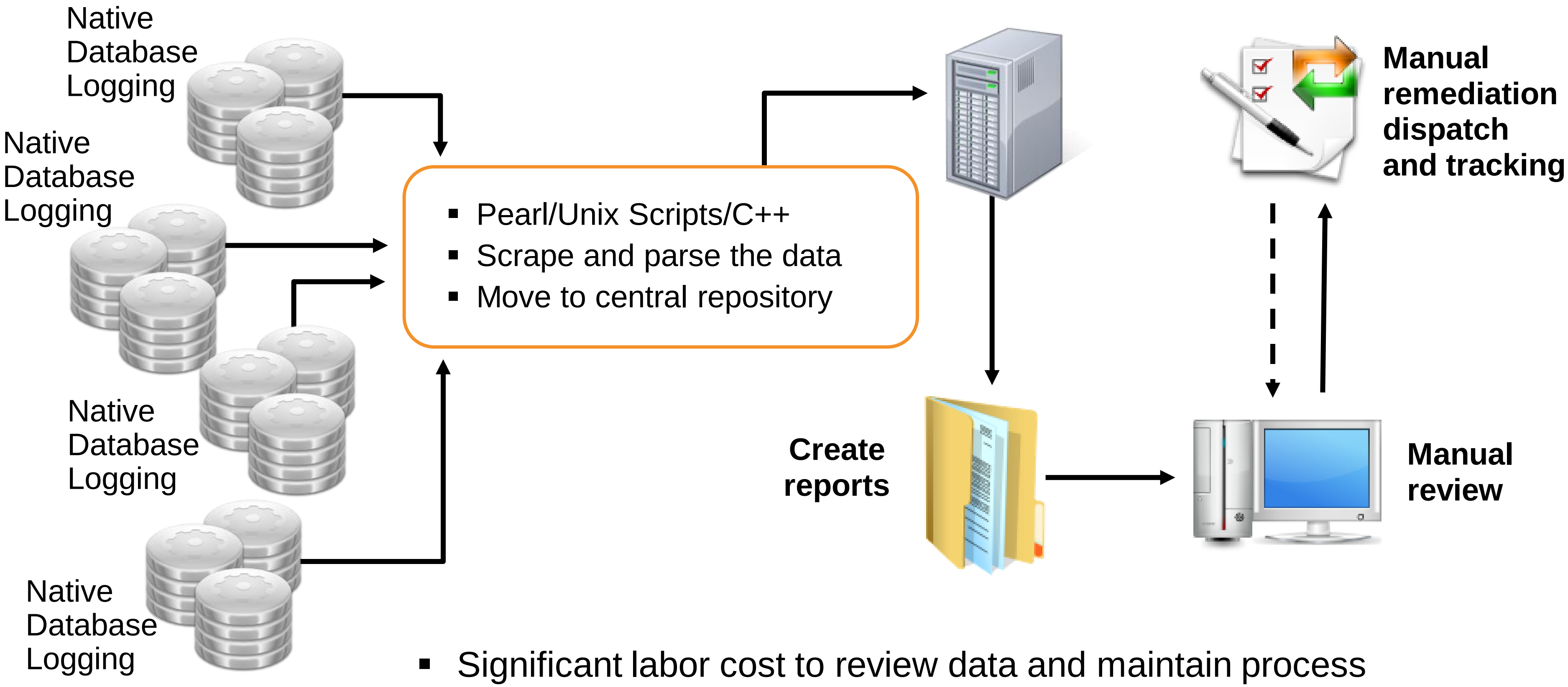
   Automated, continuous controls

   Simplified audits

   Minimal performance impact

   No changes to databases or applications

# What Database Audit Tools are Enterprises Using Today?



Native Database Logging

Native Database Logging

Native Database Logging

Native Database Logging

- Pearl/Unix Scripts/C++
- Scrape and parse the data
- Move to central repository

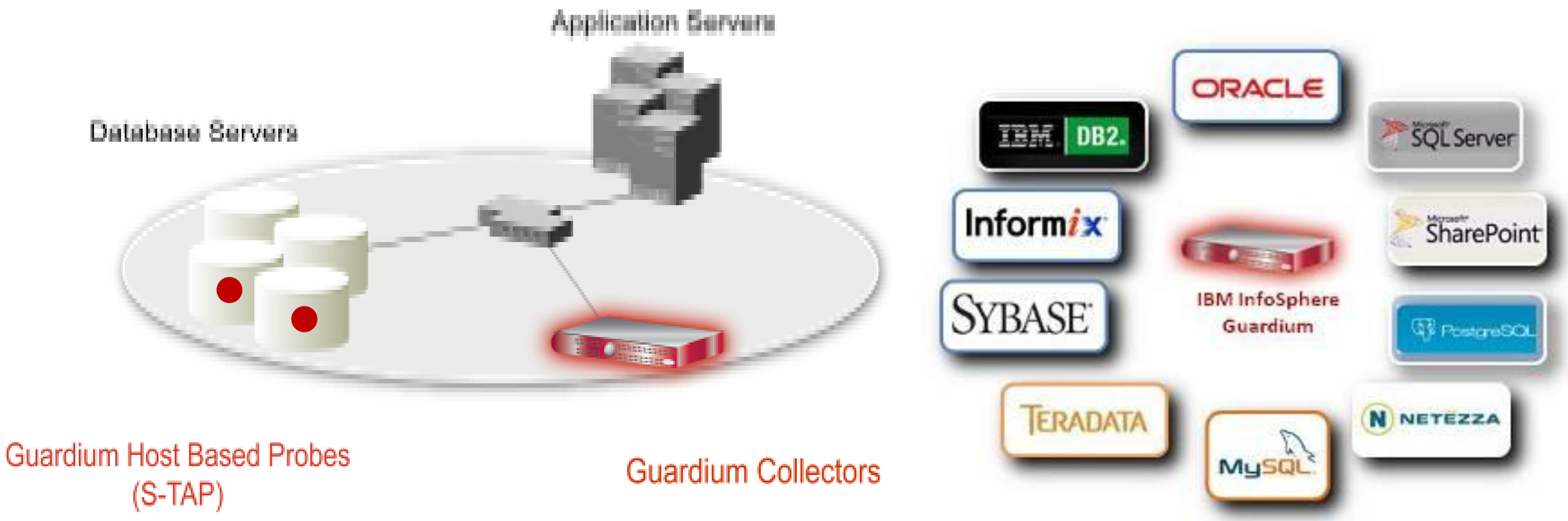
**Create reports**

**Manual review**

**Manual remediation dispatch and tracking**

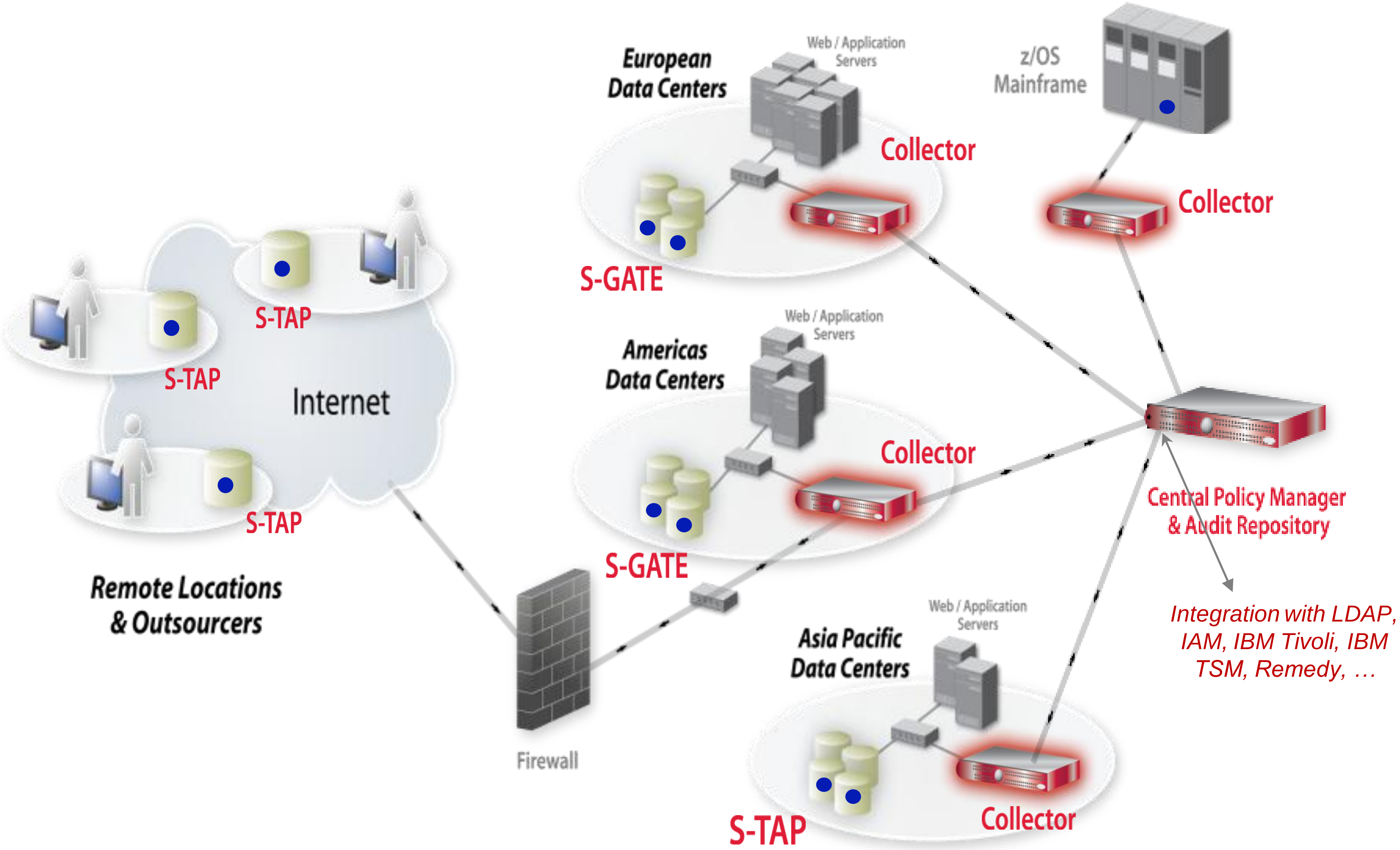
- Significant labor cost to review data and maintain process
- High performance impact on DBMS from native logging
- Not real time
- Does not meet auditor requirements for Separation of Duties
- Audit trail is not secure
- Inconsistent policies enterprise-wide

# Non-Invasive, Real-Time Database Security & Monitoring



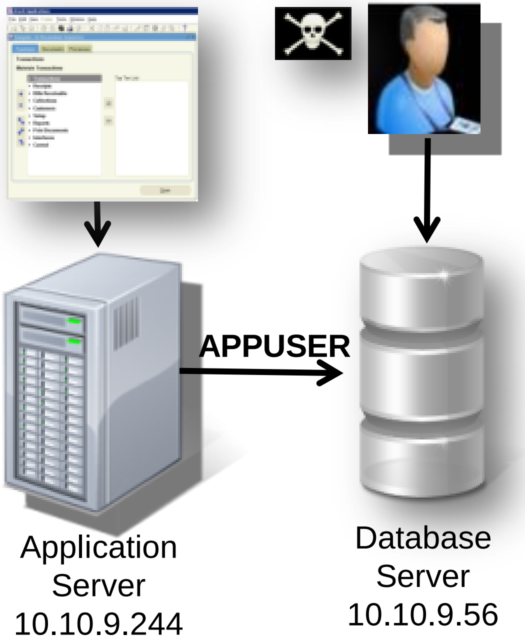
- Continuously monitors all database activities (including local access by superusers)
- Heterogeneous, cross-DBMS solution
- Does not rely on native DBMS logs
- Minimal performance impact (2-3%)
- No DBMS or application changes
- Supports Separation of Duties
- Activity logs can’t be erased by attackers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

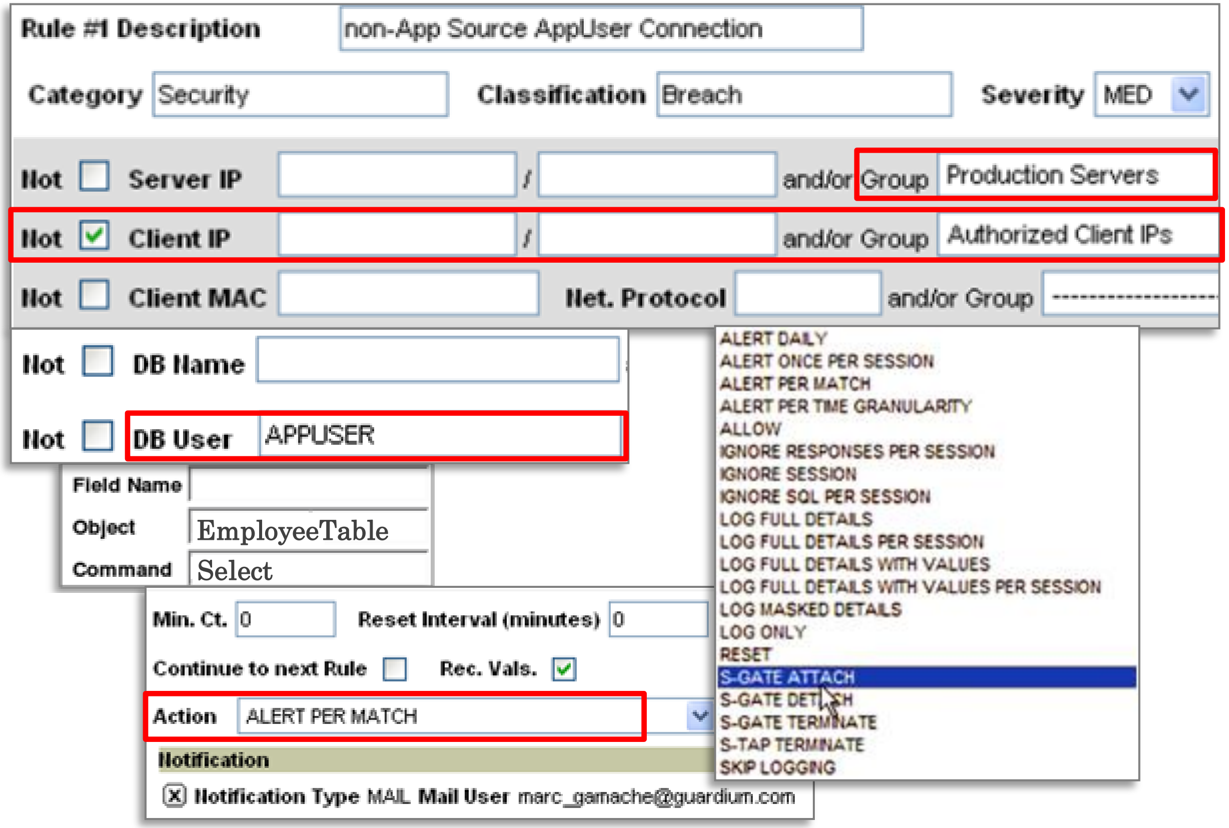
# Federated System Design



*Integration with LDAP, IAM, IBM Tivoli, IBM TSM, Remedy, …*

# 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: EmployeeTable

Command: Select

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

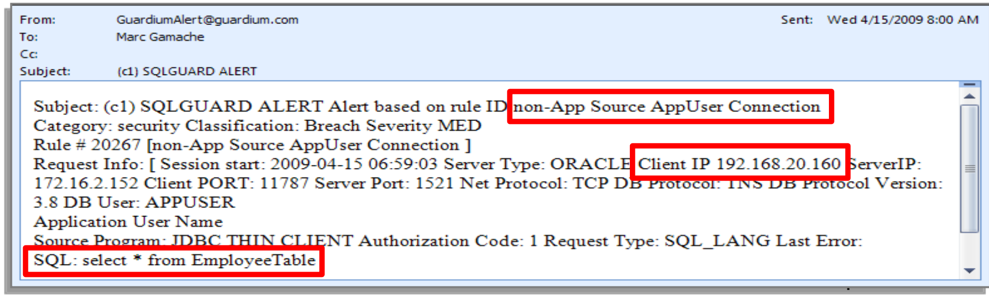
Continue to next Rule □    Rec. Vals. ☑

Action: ALERT PER MATCH

Notification

☒ Notification Type MAIL Mail User marc_gamache@guardium.com

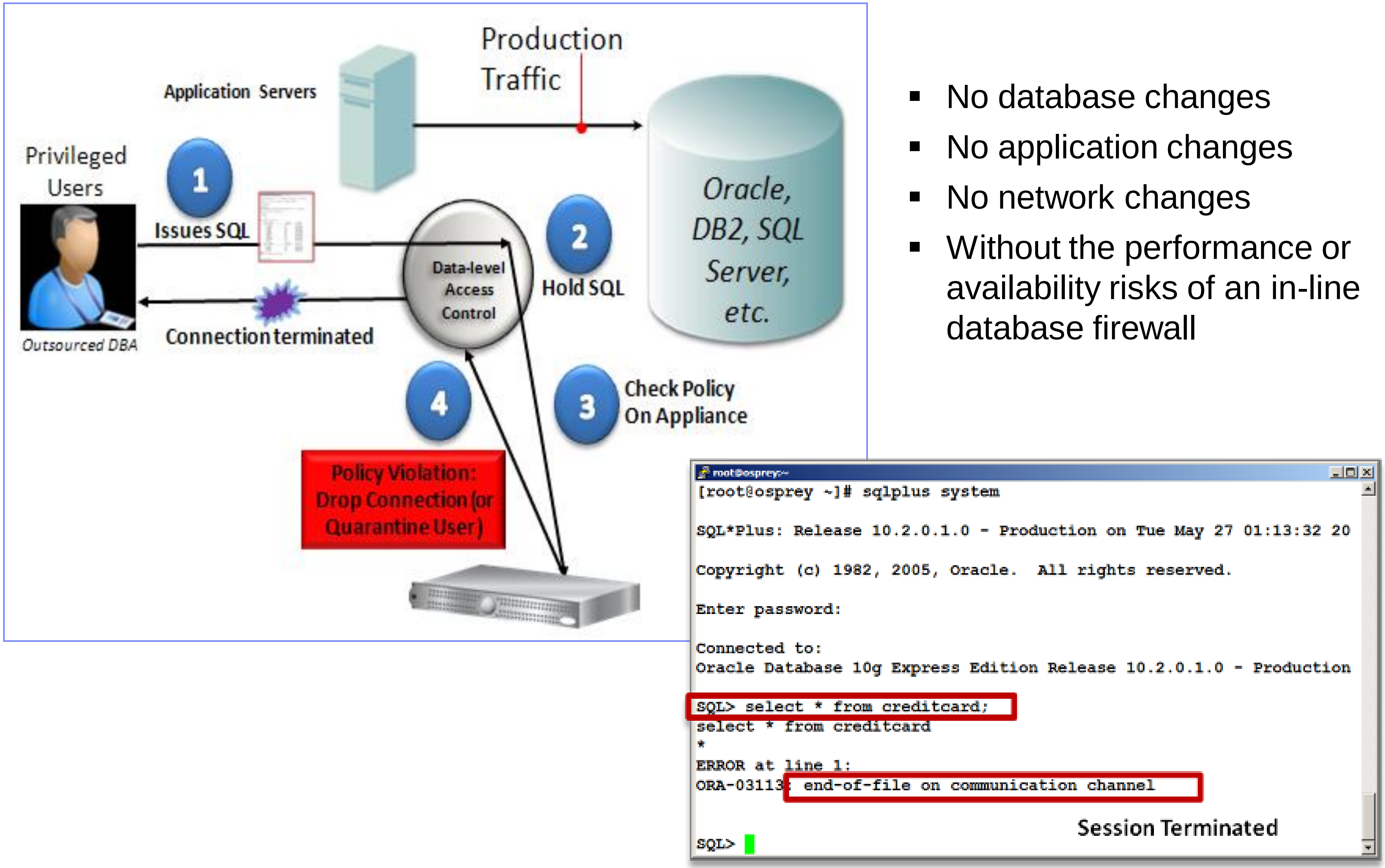
***Sample Alert***



From: GuardiumAlert@guardium.com    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

# Prevent policy violations in real-time (blocking)



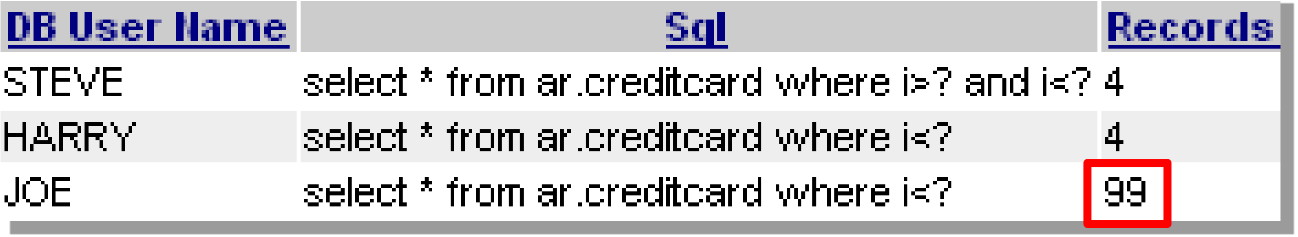
```
[root@osprey ~]# sqlplus system

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>
```

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

# Controlling Data Leakage Through Authorized Users

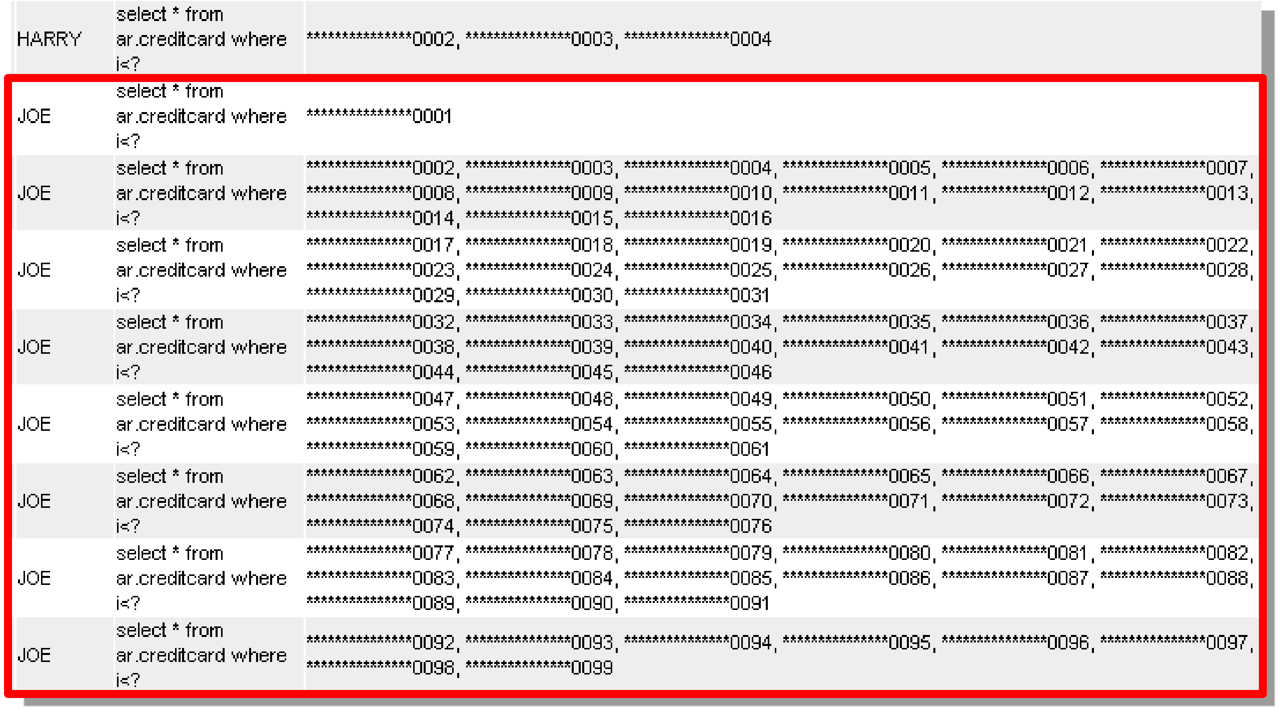
*Should my CSR view 99 records in an hour?*

**Is this normal?**



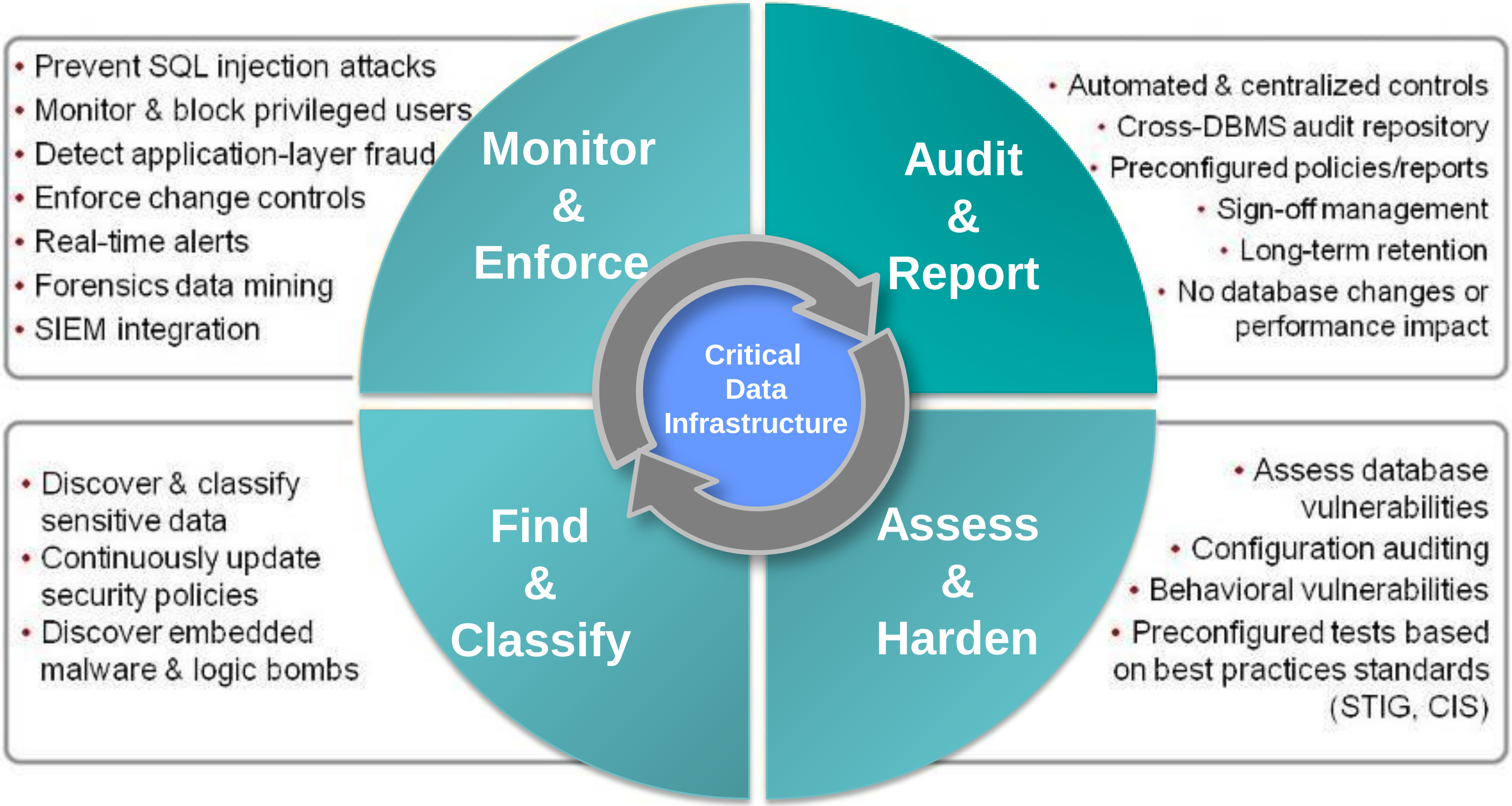
| DB User Name | Sql | Records |
|---|---|---|
| STEVE | select * from ar.creditcard where i>? and i<? | 4 |
| HARRY | select * from ar.creditcard where i<? | 4 |
| JOE | select * from ar.creditcard where i<? | 99 |

**What exactly did Joe 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 |

# Functional Modules



- Prevent SQL injection attacks
- Monitor & block privileged users
- Detect application-layer fraud
- Enforce change controls
- Real-time alerts
- Forensics data mining
- SIEM integration

- Automated & centralized controls
- Cross-DBMS audit repository
- Preconfigured policies/reports
- Sign-off management
- Long-term retention
- No database changes or performance impact

- Discover & classify sensitive data
- Continuously update security policies
- Discover embedded malware & logic bombs

- Assess database vulnerabilities
- Configuration auditing
- Behavioral vulnerabilities
- Preconfigured tests based on best practices standards (STIG, CIS)

# Simplifying Enterprise Security for Dell

CASE STUDY: SECURITY SOLUTIONS

HOW THE GUARDIUM PLATFORM HELPED DELL IT SIMPLIFY ENTERPRISE SECURITY

Safeguarding data is critical for many organizations, but auditing data access activity to comply with regulatory standards can be a complex undertaking. As part of its initiative to simplify IT, the Dell IT group implemented the Guardium platform and database activity monitoring technology to help protect its globally distributed database servers and streamline compliance processes.

*Published case study in Dell Power Solutions*

## Need:

- Improve database security for SOX, PCI & SAS70
- Simplify & automate compliance controls

## Guardium Deployment:

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

## Environment :

- Oracle & SQL Server on Windows, Linux; Oracle RAC, SQL Server clusters
- Oracle EBS, JDE, Hyperion plus in-house applications

**Previous Solution:** Native logging (MS) or auditing (Oracle) with in-house scripts

- Supportability issues; DBA time required; massive data volumes; SOD issues.

**Results:** Automated compliance reporting; real-time alerting; centralized cross-DBMS policies; closed-loop change control with Remedy integration

- Guardium “successfully met Dell’s requirements without causing outages to any databases; produced a significant reduction in auditing overhead in databases.”

# Top 5 Global Bank with Multiple Business Units

**Who:** Major global bank with multiple business units via mergers & acquisitions

- Retail & corporate banking
- Investment banking
- Mortgage banking

**Need:** Ensure privacy & integrity of all critical enterprise data

- Financial & HR data; ERP data; credit card data; PII; strategic & intellectual property
- Address PCI (Reqts. 3, 6 & 10); SOX; international data privacy laws; internal standards

**Environment**

- Oracle, SQL Server, Sybase, DB2 UDB; DB2 on z & iSeries; Informix; MySQL; Teradata
- Solaris, HP-UX, AIX, Windows, Linux
- Now monitoring ~2,000 database instances

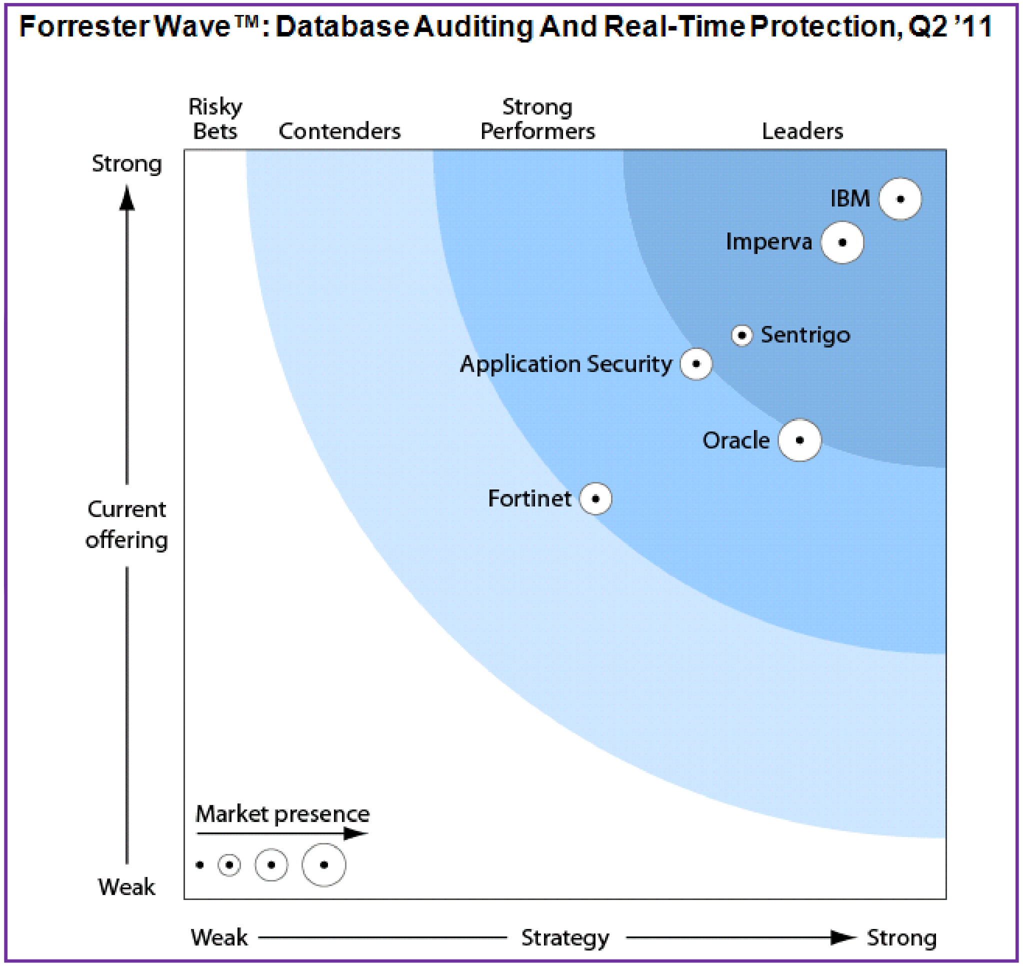
**Alternatives considered**

- Native logging/auditing from Oracle
- Symantec/ESM plus products from smaller vendors

**Results**

- Saving $1.5M per year in storage costs alone (for native audit trails)
- Guardium now a standard part of bank infrastructure
- Culture change – awareness of data security
- New processes to investigate insider threats

# InfoSphere Guardium continues to demonstrate its leadership …



Forrester Wave™: Database Auditing And Real-Time Protection, Q2 '11

2007

2011

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.

SmarterAnalytics

# Information Lifecycle Management

## *Optim Data Growth Solution*

# Organizations need a strategy to manage data throughout its life-cycle from requirements to retirement independent of applications

*Life-Cycle Management involves managing data growth and application performance which otherwise has many negative organizational consequences:*

**Enterprise applications perform slowly**

- Batch jobs run into working hours, impacting end-user productivity & missed SLAs
- Customer satisfaction declining

**As the size of the production instance grows, so do back-up & non-production systems**

- If a failure occurs, how long will a database recovery take?
- How many copies of data are being maintained?

**New application functionality to meet business needs is not deployed on schedule**

- Test environments take longer long to setup
- Sensitive data can be inadvertently exposed when cloning method used

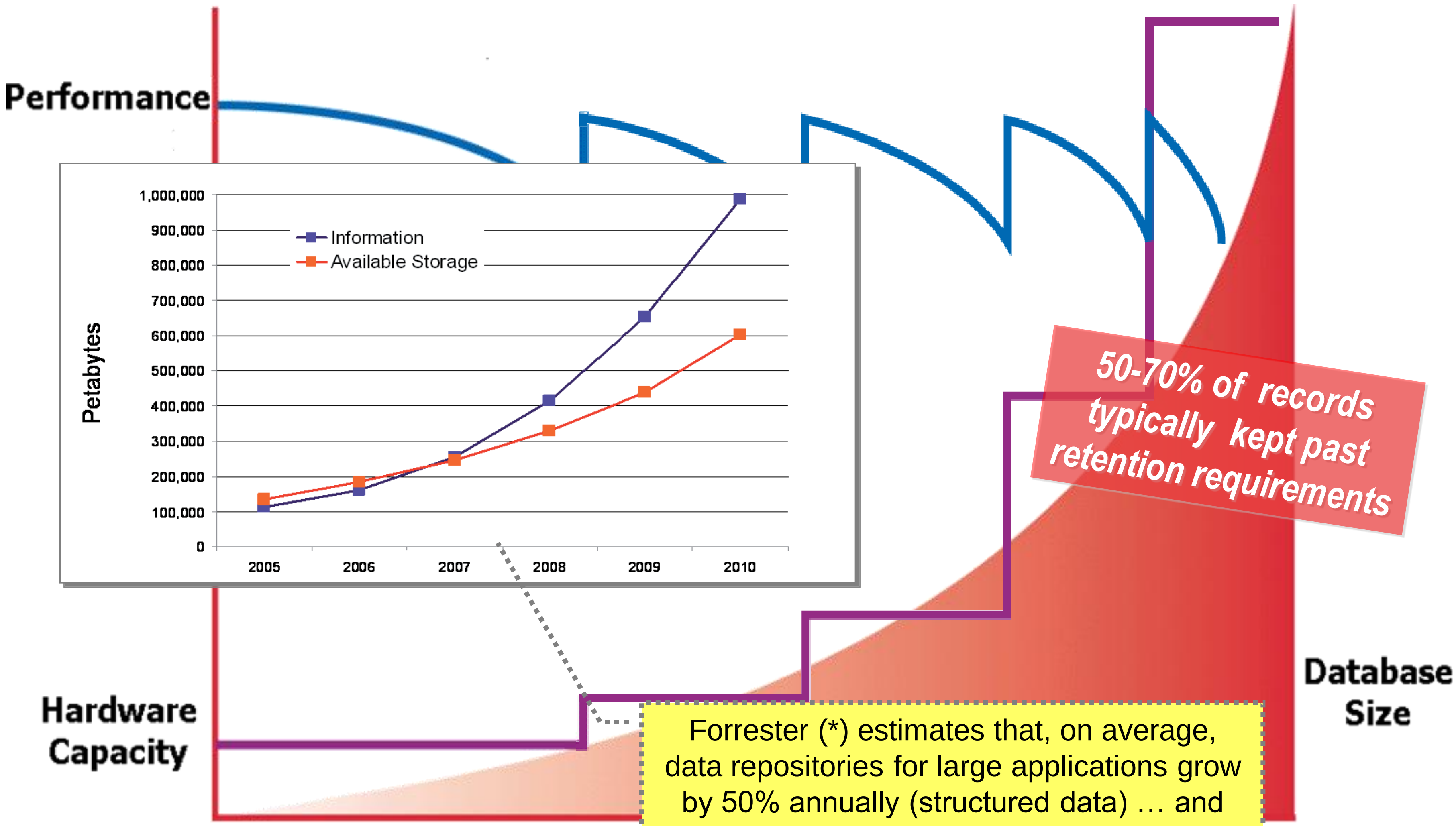
**Potential liability of keeping data beyond the data retention rules**

- How to access data from legacy or unsupported systems?

**Increased infrastructure & storage costs**

- “Every time I turn around, we are buying more storage”

# Explosive Data Growth



50-70% of records typically kept past retention requirements

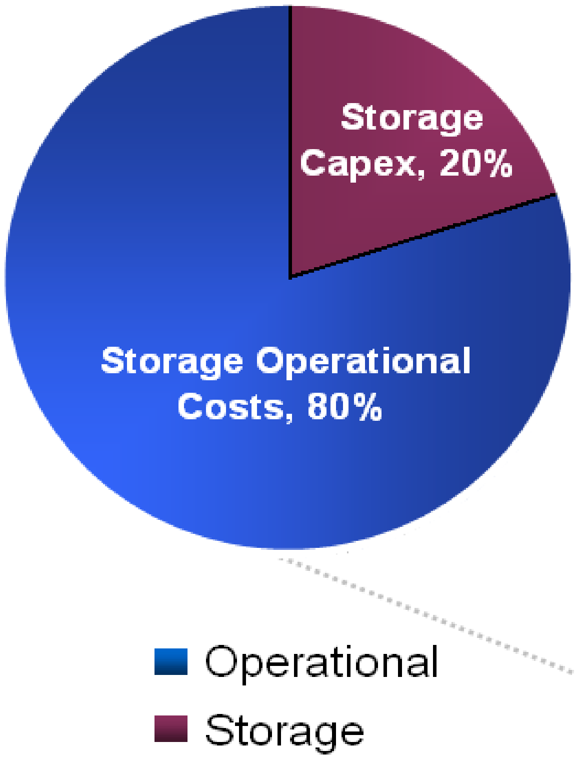
Forrester (*) estimates that, on average, data repositories for large applications grow by 50% annually (structured data) … and 85% of data stored in databases is inactive

* Source: Noel Yuhanna, Forrester Research, Database Archiving Remains An Important Part Of Enterprise DBMS Strategy

# The results can have significant financial impact

ge systems

Industry Average Fully Burdened IT Infrastructure Cost Percentages to support data growth



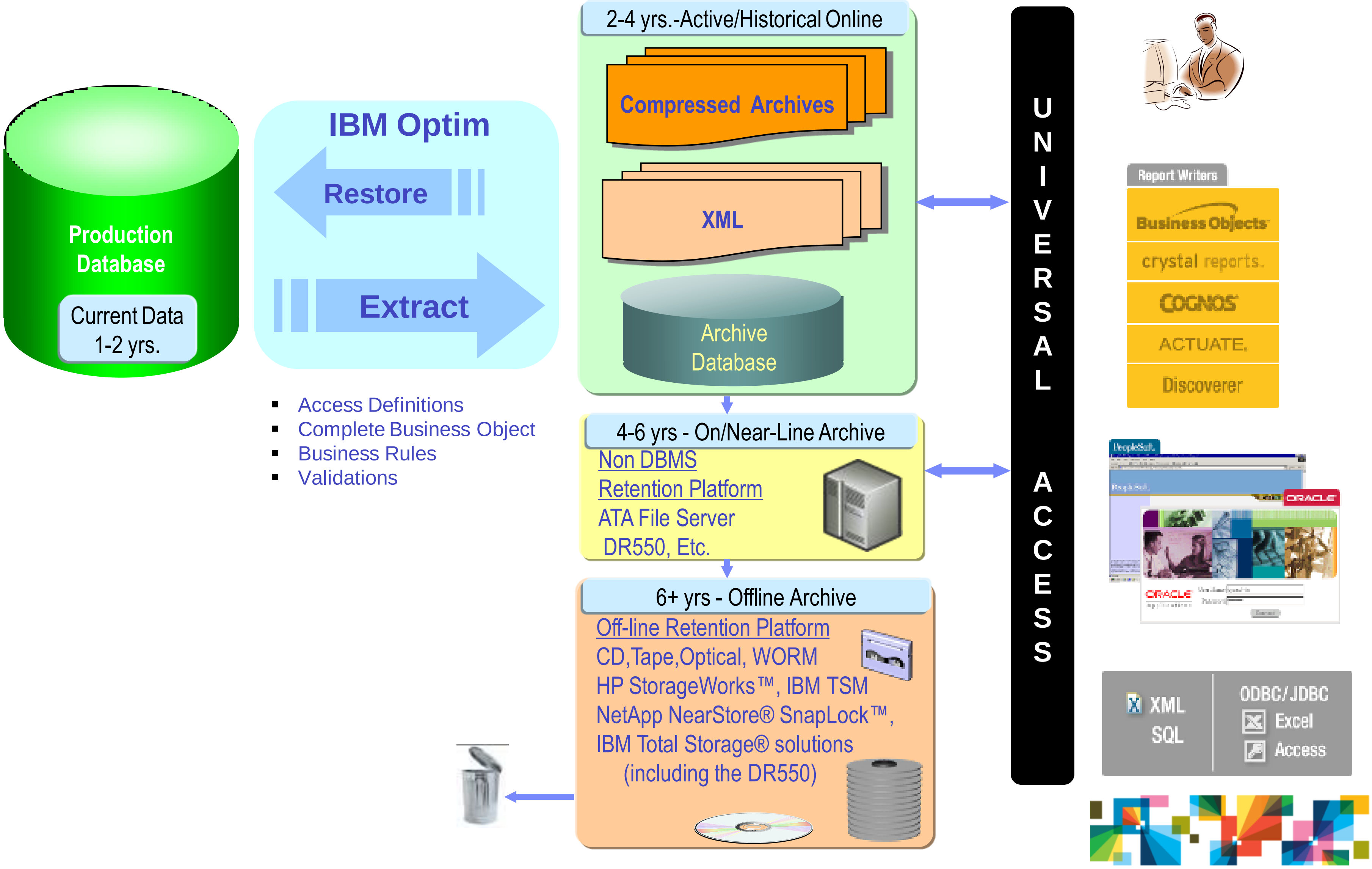
M

A

| Industry Averages | |
|---|---|
| Type | Industry Average |
| Disk Storage + Tape | 20% |
| Hardware: Networking (cables, routers, etc) | 15% |
| Software (for storage) | 17% |
| Infrastructure: Telcom | 10% |
| Infrastructure: Power | 5% |
| Infrastructure: Floor Space | 3% |
| Staffing (for storage) | 30% |
| **Total** | **100%** |

For every 20% that is spent on storage, 80% cost is spent on the operational elements of managing that stored information

# Optim Data Growth Solution Overview



Production Database

Current Data 1-2 yrs.

IBM Optim

Restore

Extract

- Access Definitions
- Complete Business Object
- Business Rules
- Validations

2-4 yrs.-Active/Historical Online

Compressed Archives

XML

Archive Database

4-6 yrs - On/Near-Line Archive

Non DBMS
Retention Platform
ATA File Server
DR550, Etc.

6+ yrs - Offline Archive

Off-line Retention Platform
CD,Tape,Optical, WORM
HP StorageWorks™, IBM TSM
NetApp NearStore® SnapLock™,
IBM Total Storage® solutions
(including the DR550)

UNIVERSAL ACCESS

Report Writers

Business Objects

crystal reports.

COGNOS

ACTUATE.

Discoverer

XML
SQL

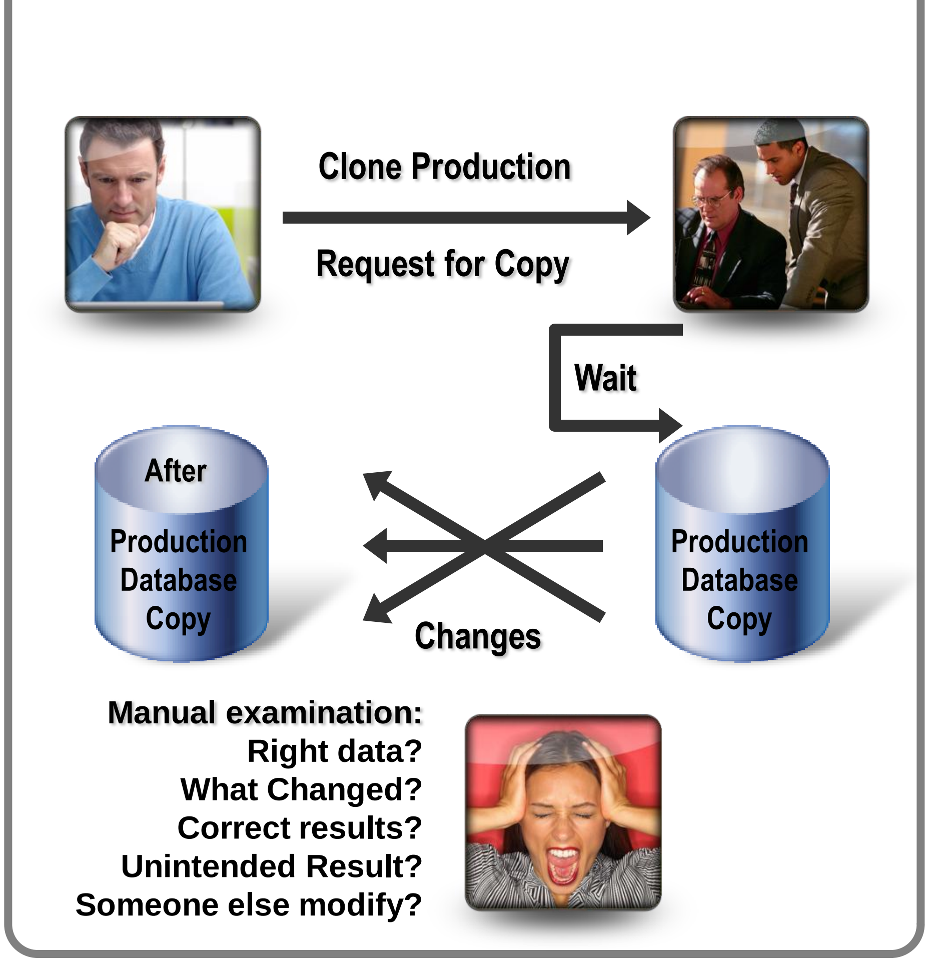
ODBC/JDBC
Excel
Access

# Information Lifecycle Management

## *Optim Test Data Management & Data Masking Solution*

# Test Data Management - Current Approaches

## #1 - Clone Production



Clone Production

Request for Copy

Wait

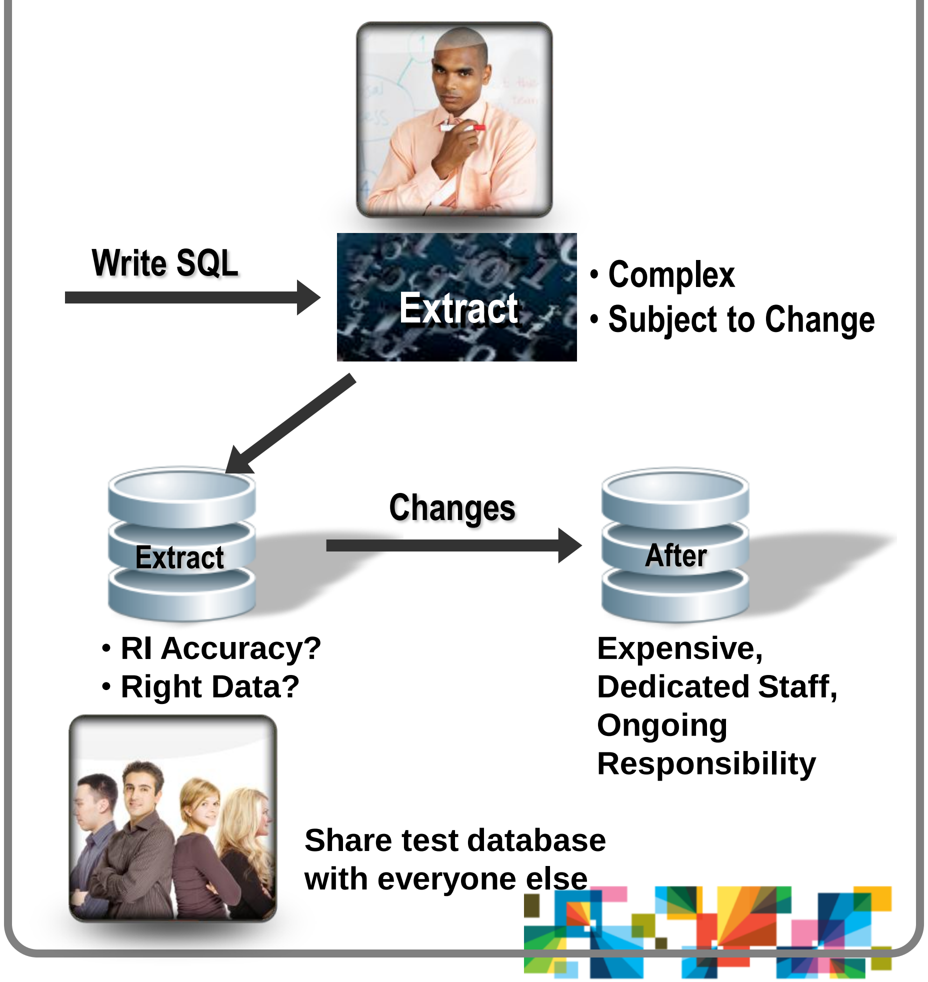
After Production Database Copy

Production Database Copy

Changes

Manual examination:
Right data?
What Changed?
Correct results?
Unintended Result?
Someone else modify?

## #2 – Write SQL



Write SQL

Extract

- Complex
- Subject to Change

Extract

Changes

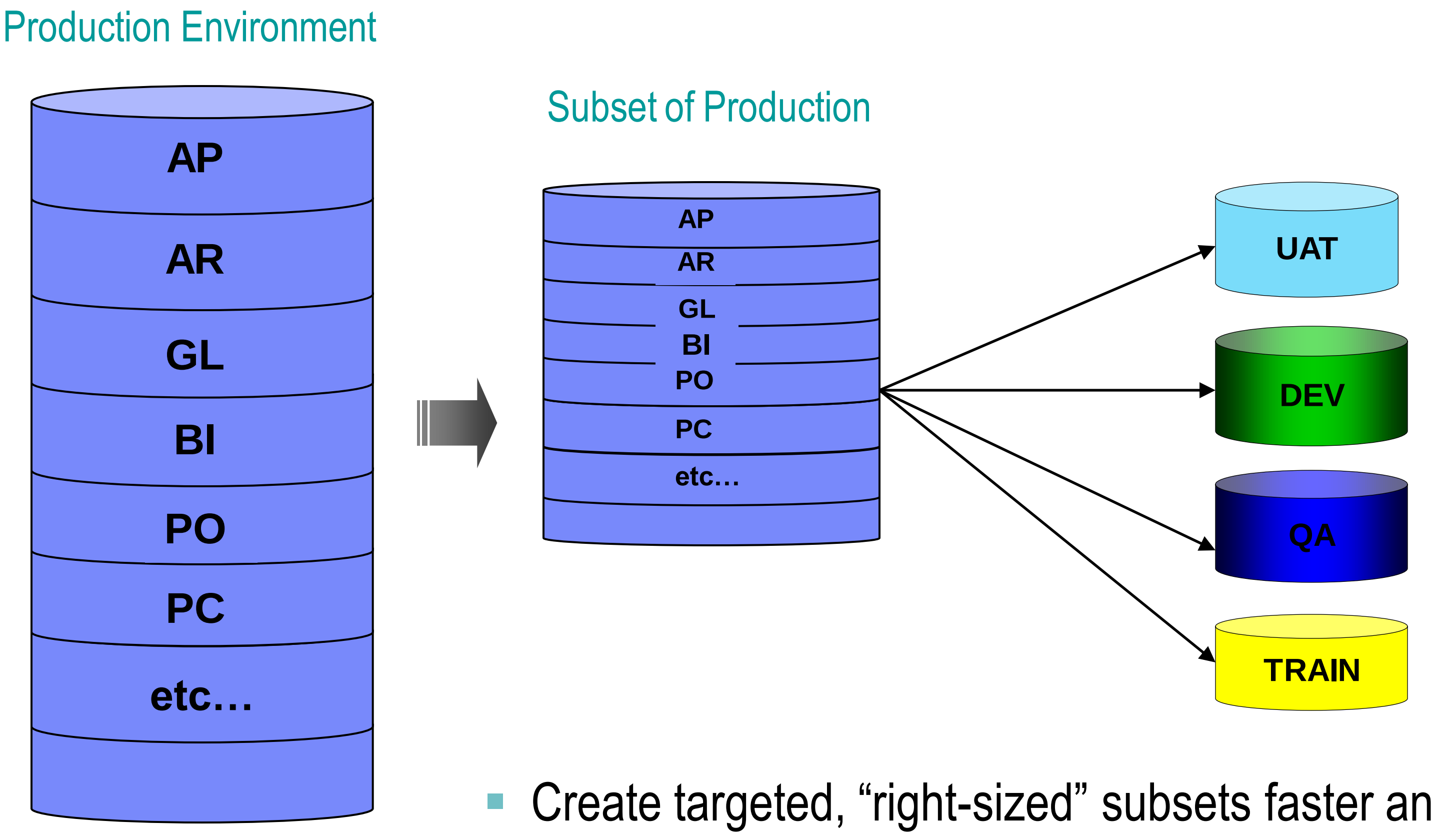
After

- RI Accuracy?
- Right Data?

Expensive,
Dedicated Staff,
Ongoing
Responsibility

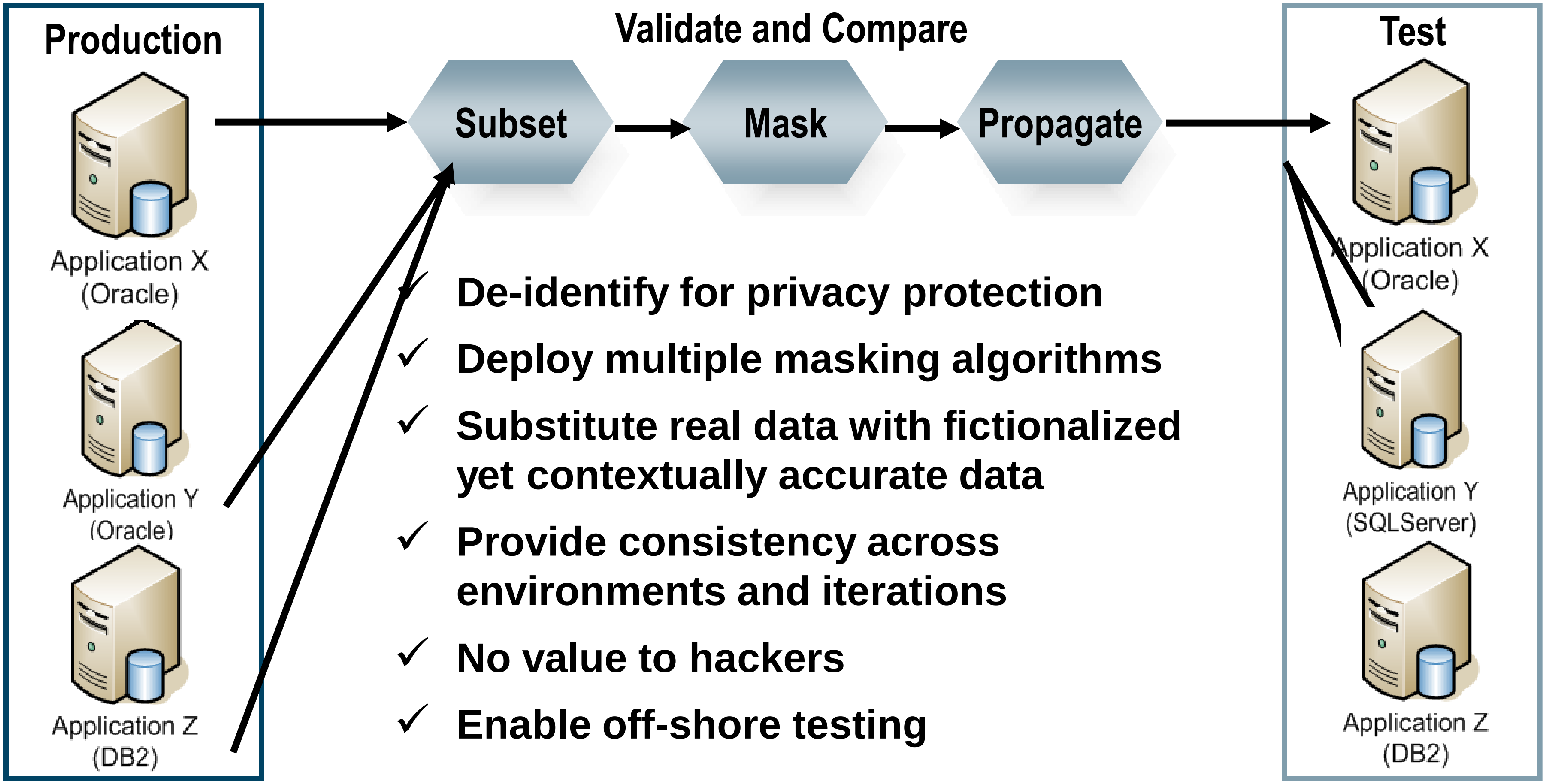
Share test database
with everyone else

# Test Data Management using Subsetting:



- Create targeted, “right-sized” subsets faster and more efficiently than cloning
- Compare to pinpoint and resolve application defects faster
- Improve development efficiencies

# Optim Data Privacy with TDM



- ✓ **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**

# Optim Data Privacy

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

### Patient Information

**Patient No.** 123456 **SSN** 333-22-4444

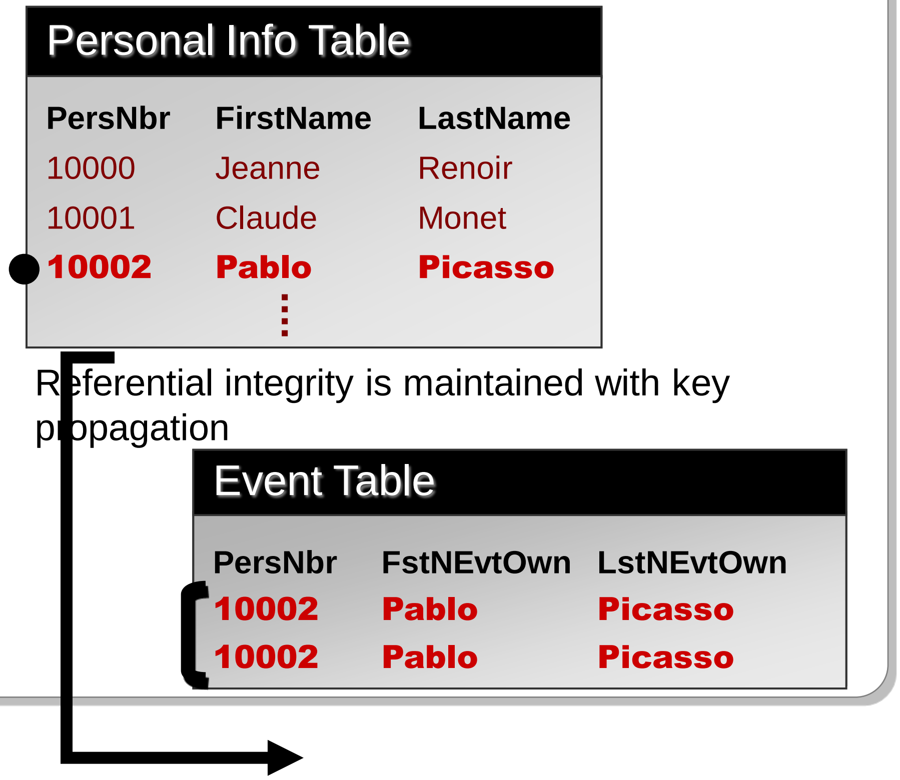
**Name** Erica Schafer

**Address** 12 Murray Court

**City** Austin **State** TX **Zip** 78704

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

## Example 2



### Personal Info Table

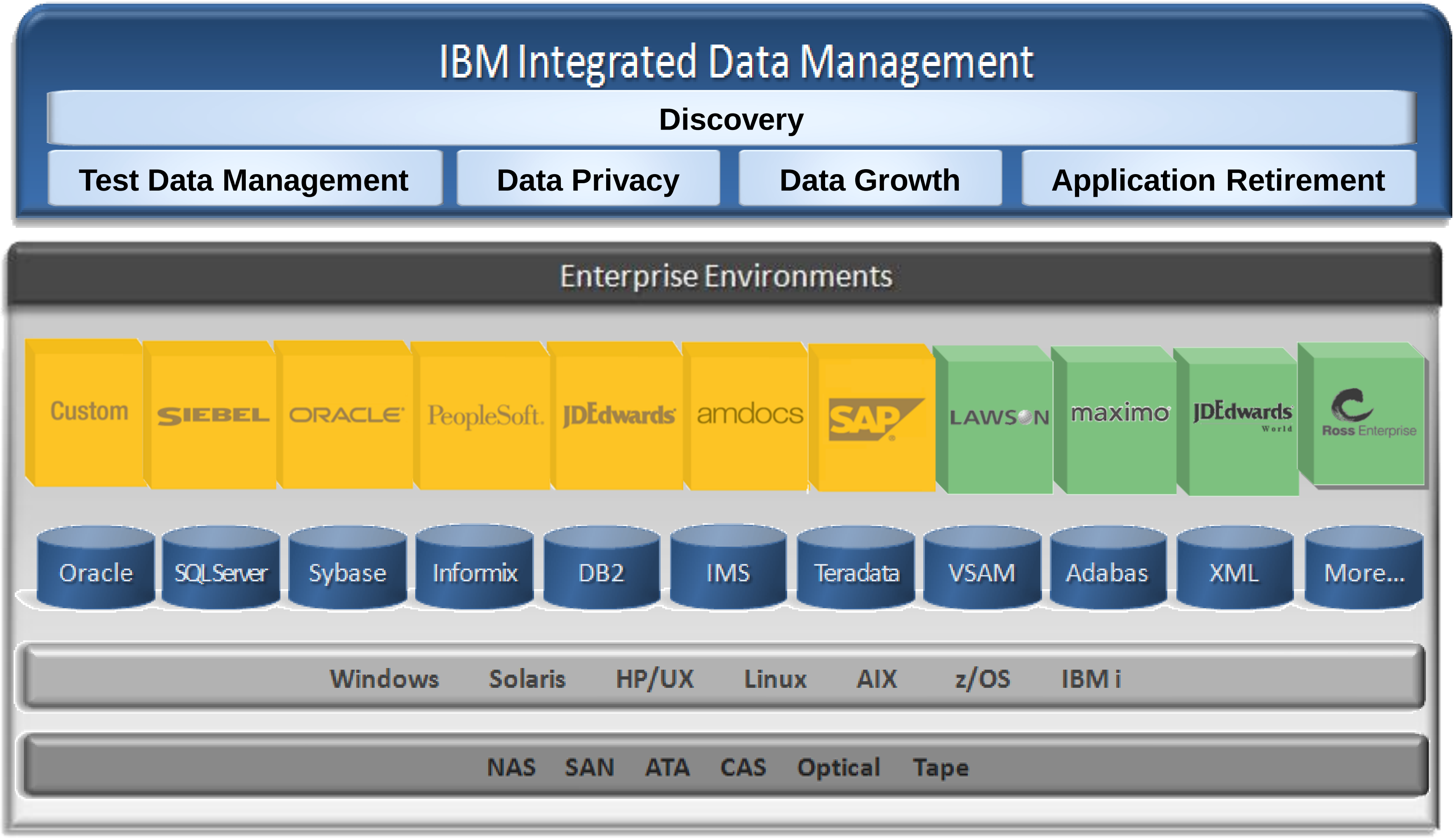
| PersNbr | FirstName | LastName |
|---|---|---|
| 10000 | Jeanne | Renoir |
| 10001 | Claude | Monet |
| **10002** | **Pablo** | **Picasso** |
| ⋮ | | |

Referential integrity is maintained with key propagation

### Event Table

| PersNbr | FstNEvtOwn | LstNEvtOwn |
|---|---|---|
| **10002** | **Pablo** | **Picasso** |
| **10002** | **Pablo** | **Picasso** |

# Infosphere Optim Enterprise Architecture



IBM Integrated Data Management

Discovery

Test Data Management | Data Privacy | Data Growth | Application Retirement

Enterprise Environments

Custom, SIEBEL, ORACLE, PeopleSoft, JDEdwards, amdocs, SAP, LAWSON, maximo, JDEdwards World, Ross Enterprise

Oracle, SQLServer, Sybase, Informix, DB2, IMS, Teradata, VSAM, Adabas, XML, More…

Windows, Solaris, HP/UX, Linux, AIX, z/OS, IBM i

NAS, SAN, ATA, CAS, Optical, Tape

**Single, scalable, interoperable data management solution provides a central point to deploy policies to extract, store, port, and protect application data records from creation to deletion**

# Name 2 IBM Solutions that support Data Security and Compliance

➡

1. InfoSphere Guardium & Optim
2. Lotus Messaging & Websphere Application Server
3. DB2 & Lotus Symphony

Thank
You