Pulse

IBM SolutionsConnect 2013

Implementing Database Security and Auditing Against Data Breaches

Stephen Cottrell

Data Governance Lead of Optim & Guardium,
IBM Asia Pacific

IBM

What we'll discuss

- Information Governance Overview
- Protecting Sensitive Data – Challenges
- What's at Stake?
- Ensuring Information Security and Privacy
  - Understand & Define
  - Secure & Protect
  - Monitor & Audit
- Client success with IBM Solutions for InfoSphere Information Governance

A Smarter Planet harnesses today's information explosion for business benefit…

Instrumented

Interconnected

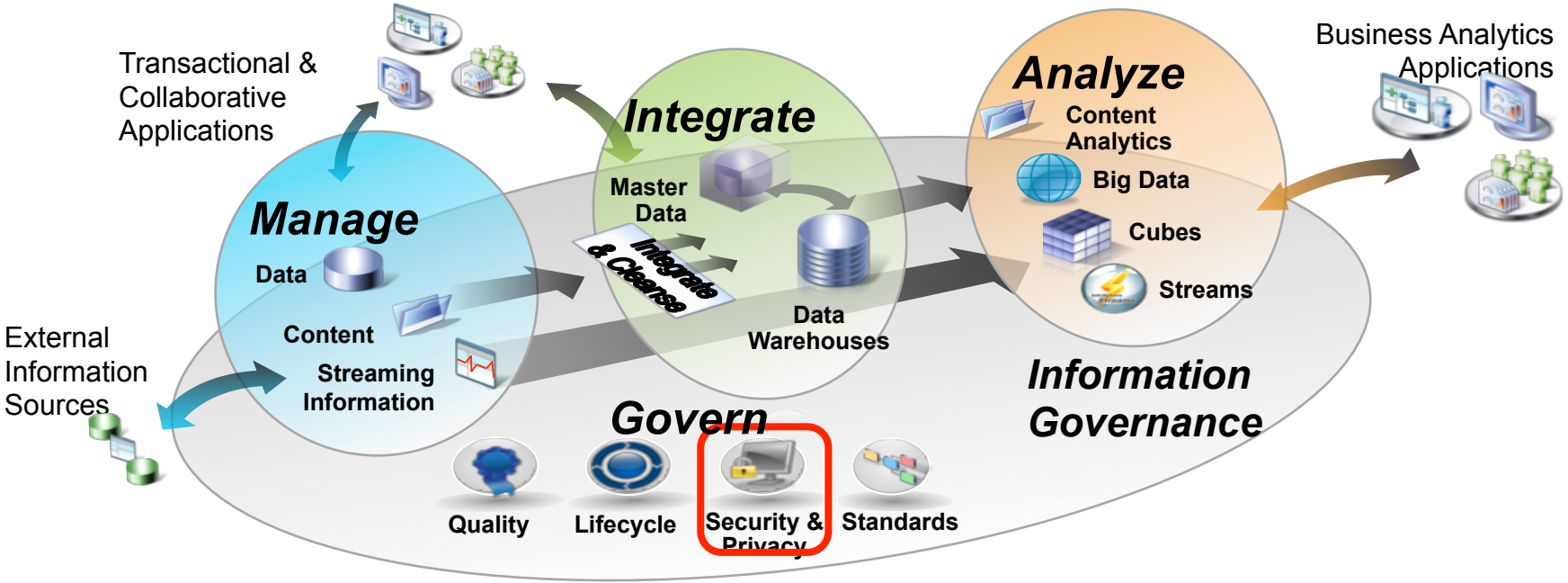
Intelligent

… creating a need for better Information Governance

- Streamlining processes to manage business growth with consistency
- Ensuring compliance with policies, laws and regulations
- Controlling costs and optimizing infrastructure

Information governance is the orchestration of people, process and technology to enable an organization to leverage information as an enterprise asset.

Mastering information across the Information Supply Chain



Trusted ◆ Relevant ◆ Governed

Keeping up with ever-changing global and industry regulations

Proposed Law from European Commission

"…Organizations that fail to issue notifications about a personal data breach in a timely or complete fashion to the supervisory authority will face fines of up to 2 percent of their current revenues…"

Source: ComputerWorld Hong Kong Daily Newsletter on Jan 27, 2012

Personal Data (Privacy) Ordinance – Hong Kong

Data Protection Principles

- **Principle 1** -- Purpose and manner of collection
  This provides for the lawful and fair collection of personal data and sets out the information a data user must give to a data subject when collecting personal data from that subject.
- **Principle 2** -- Accuracy and duration of retention
  This provides that personal data should be accurate, up-to-date and kept no longer than necessary.
- **Principle 3** -- Use of personal data
  This provides that unless the data subject gives consent otherwise personal data should be used for the purposes for which they were collected or a directly related purpose.
- **Principle 4** -- Security of personal data
  This requires appropriate security measures to be applied to personal data (including data in a form in which access to or processing of the data is not practicable).
- **Principle 5** -- Information to be generally available
  This provides for openness by data users about the kinds of personal data they hold and the main purposes for which personal data are used.
- **Principle 6** -- Access to personal data
  This provides for data subjects to have rights of access to and correction of their personal data.

From http://www.pcpd.org.hk/english/ordinance/ordglance1.html#dataprotect

What's the risk?

Hackers obtained personal information on 70 million subscribers.

April 2011: *Malicious outsiders stole name, address (city, state, zip), country, email address, birth date, PlayStation Network/Qriocity password and login, and handle/PSN online ID, and possibly credit card numbers from 70 million Sony PlayStation users.*

SQL injection is fast becoming one of the biggest and most high profile web security threats.

April 2011*: A mass SQL injection attack that initially compromised 28,000 websites shows no sign of slowing down. Known as LizaMoon, this malicious code is after anything stored in a database.*

Unprotected test data sent to and used by test/development teams as well as third-party consultants.

February 2009: *An FAA server used for application development & testing was breached, exposing the personally identifiable information of 45,000+ employees.*

Hundreds of thousands of secret reports regarding US wars in Iraq and Afghanistan published on WikiLeaks.

December 2010: *A private in the US military, downloaded top secret military documents and passed them to journalist for publication. This puts US national security at risk as well as the lives of those named in reports.*

Organisations face difficult decisions

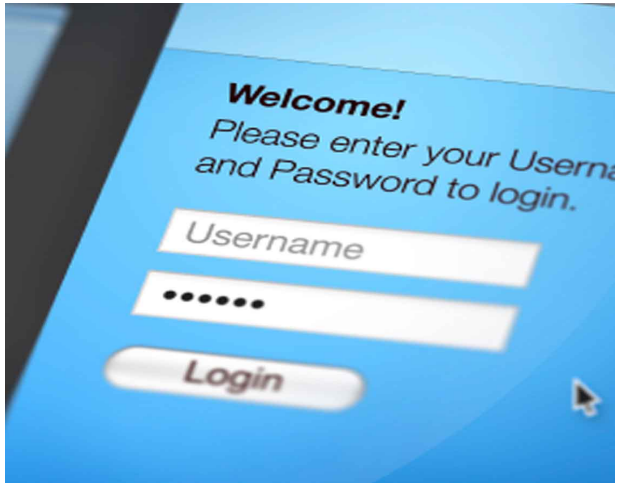
- **Do nothing** … however:
  - Limited time, lots of regulation, growing costs of compliance
  - Requirements for privacy/security by user role add complexity
  - **73%** of security professionals say the volume of database attacks will increase
  - **$7.2M USD** is the average cost of a data breach
  - **95%** of compromised records originated in **database servers**
  - **88%** of organizations surveyed had at least one data breach
- **Leverage home grown approaches** … however:
  - Manual approaches lead to higher risk and inefficiency
  - Requirements for privacy/security by user role add complexity
  - New source of threats: outsourcing, web-facing applications, stolen credentials, insiders

Don't focus just on one or two databases but extend your efforts to become enterprisewide — encompassing hundreds and thousands of databases.

-- Why Enterprise Database Security Strategy Has Become Critical, Forrester Research, Inc, July 13, 2011

Can today's organizations protect their information?

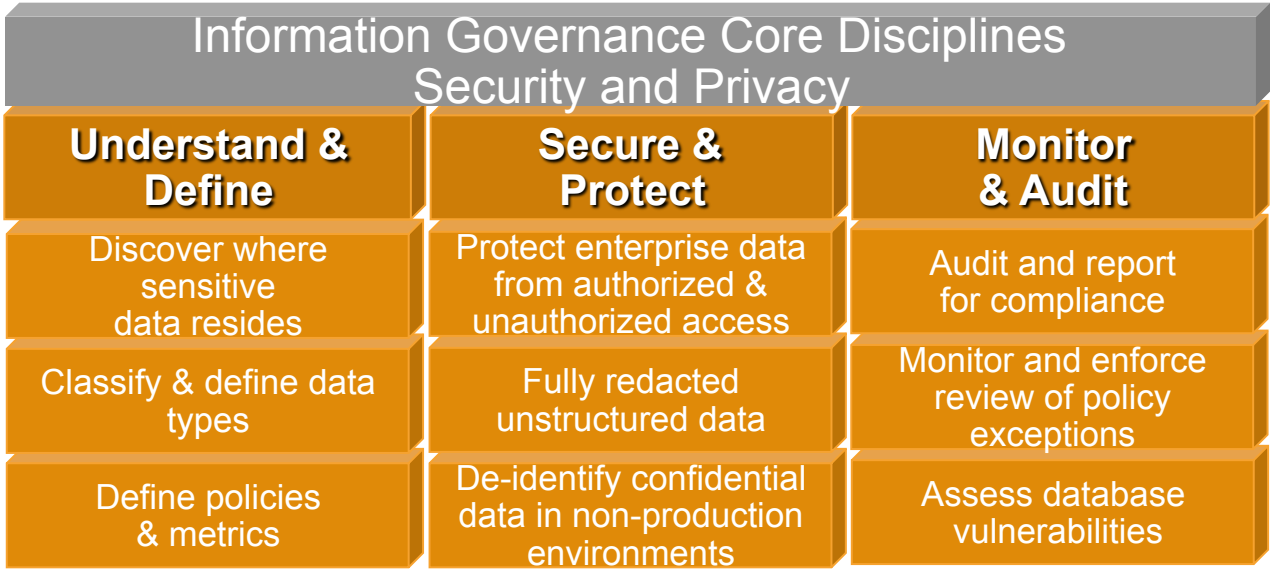
- Where does your sensitive data reside across the enterprise?
- How can your data be protected from both authorized and unauthorized access?
- Can your confidential data in documents be safeguarded while still enabling the necessary business data to be shared?
- How can access to your enterprise databases be protected, monitored and audited?
- Can data in your non-production environments



Larry Ponemon, founder of the group that bears his name, said that survey shows a shift in the way C-level executives think about security software. Investing in data protection, he said, is now seen as less expensive than recovering from a data breach.

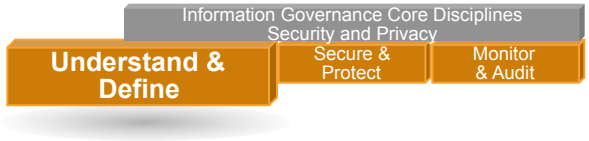
-- InformationWeek

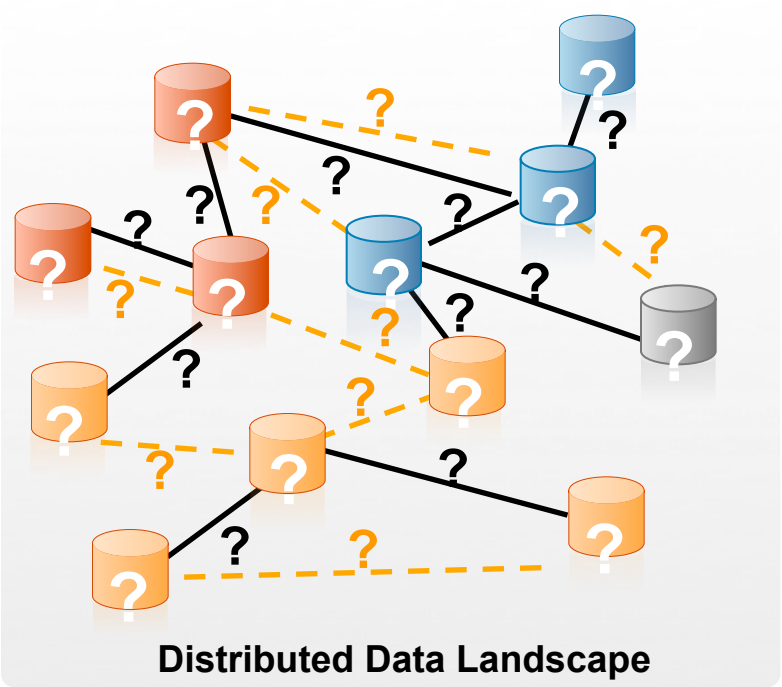
Requirements to manage the security and privacy of data



A data security strategy should include database auditing and monitoring, patch management, data masking, access control, discovery/classification, and change management. *-- Why Enterprise Database Security Strategy Has Become Critical, Forrester Research, Inc, July 13, 2011*

You can't govern what you don't understand

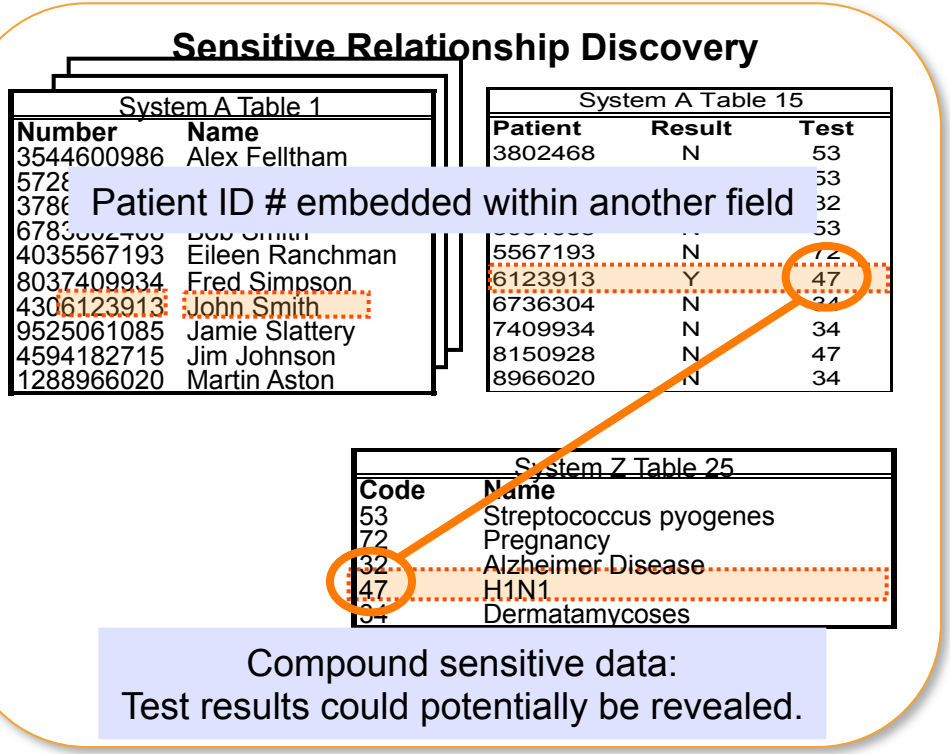


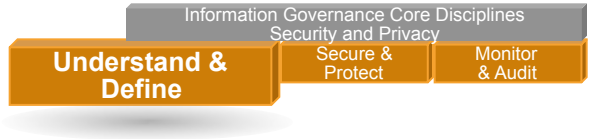


Distributed Data Landscape

- 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

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

Protection of data requires a 360-degree strategy

Protect diverse data types across the enterprise

Data in heterogeneous databases

(Oracle, DB2, Netezza, Informix, Sybase, Sun MySQL, Teradata)

- DB Activity Monitoring
- DB Vulnerability Assessment
- Data Masking
- Data Encryption

Data not in databases

(File Shares, ex. SharePoint, .TIF, .PDF, .doc, scanned documents)

- Data Redaction
- Access monitoring f… es

Data extracted from database

- Data Encryption
- Data Masking

Data in daily use

- DB Activity Monitoring
- DB Vulnerability Assessment
- Data Masking
- Data Encryption

Structured Data

Unstructured Data

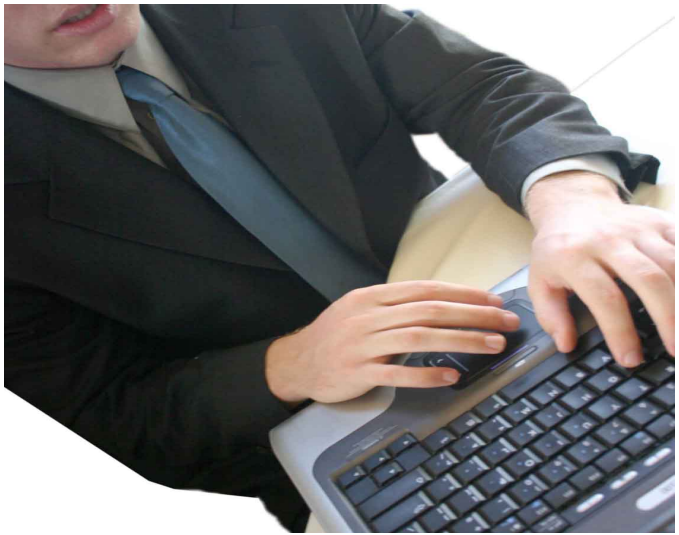
Offline Data

Online Data

Production & Non-Production Systems

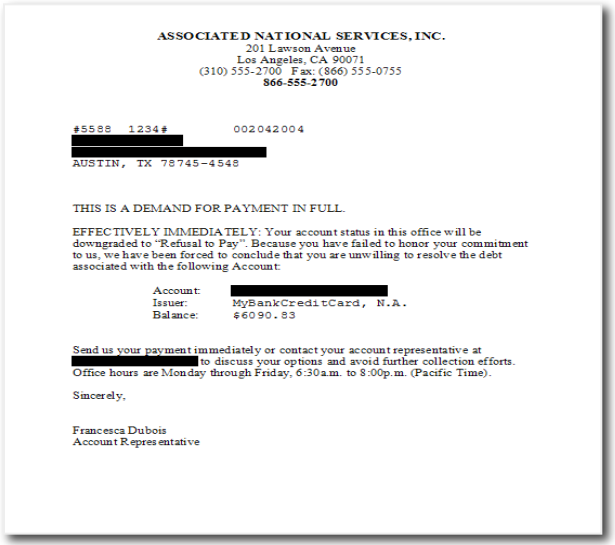
Protecting data is both an external and internal issue

- Prevent “power users” from abusing their access to sensitive data (separation of duties)
  - DBA and power users
- Prevent authorized users from misusing sensitive data
  - For example, third-party or off-shore developers
- Prevent intrusion and theft of data
  - For example, someone walking off with a back-up tape
  - Hacker
  - Database vulnerabilities (user id with no password or default password)



Protect unstructured data with redaction

Redaction: *the act or process of editing or revising a piece of writing by removing sensitive information.*



ASSOCIATED NATIONAL SERVICES, INC.
201 Lawson Avenue
Los Angeles, CA 90071
(310) 555-2700 Fax: (866) 555-0755
866-555-2700

#5588 1234# 002042004
[redacted]
AUSTIN, TX 78745-4548

THIS IS A DEMAND FOR PAYMENT IN FULL.

EFFECTIVELY IMMEDIATELY: Your account status in this office will be downgraded to "Refusal to Pay". Because you have failed to honor your commitment to us, we have been forced to conclude that you are unwilling to resolve the debt associated with the following Account:

Account: [redacted]
Issuer: MyBankCreditCard, N.A.
Balance: $6090.83

Send us your payment immediately or contact your account representative at [redacted] to discuss your options and avoid further collection efforts. Office hours are Monday through Friday, 6:30a.m. to 8:00p.m. (Pacific Time).

Sincerely,

Francesca Dubois
Account Representative

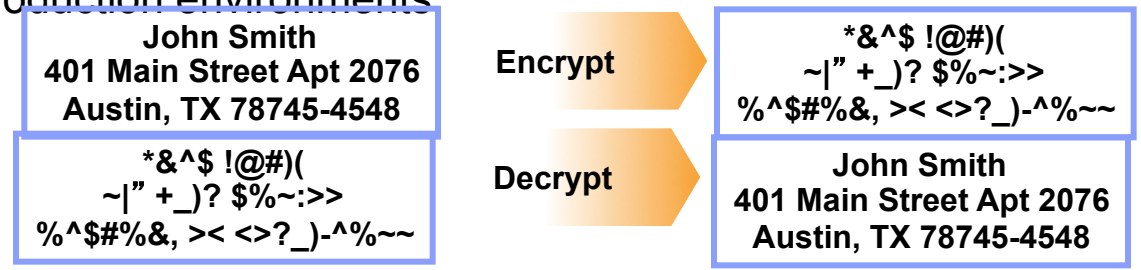
- Redaction usually happens as a result of a request, or a need to share select information
- Redaction is not a replacement for:
  - Encryption
  - Proper access control
  - Secure document lifecycle management tools

Protect sensitive structured data values with masking

- **Definition**
  *Method for creating a **structurally similar but inauthentic** version of an organization's data. The **purpose is to protect the actual data** while having a functional substitute for occasions when the real data is not required.*
- **Requirement**
  *Effective data masking requires data to be altered in a way that the **actual values cannot be determined** or reengineered, **functional appearance is maintained**.*
- **Other Terms Used**
  Obfuscation, scrambling, data de-identification
- **Commonly masked data types**
  Name, address, telephone, SSN/national identity number, credit card number
- **Methods**
  - Static Masking: *Extracts rows from production databases, obfuscating data values that ultimately **get stored in the columns in the test databases***
  - Dynamic Masking: *Masks specific data elements **on the fly** without touching applications or physical production data store*

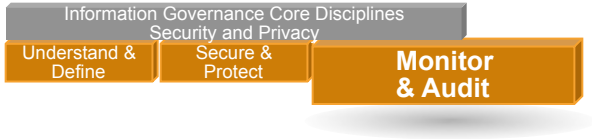
Protect online and offline data with encryption

- Encryption **transforms data to make it unreadable** except to those with a special key
- **Encrypted data is meaningless** so unauthorized access causes no harm
- **Original data is preserved** so encryption is an ideal choice for protecting production environments

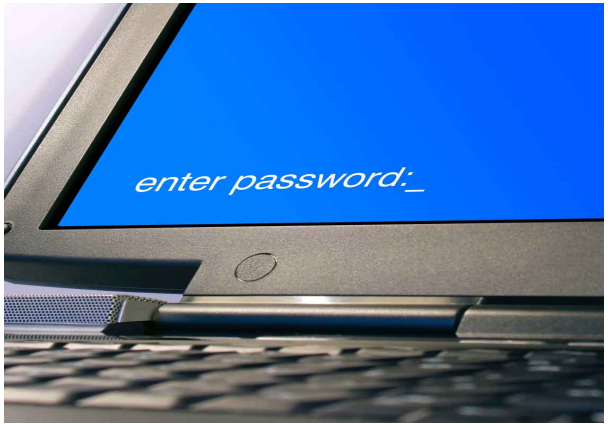


Personal identifiable information is encrypted making it meaningless without a proper key.

Streamline and simplify compliance processes



- Alerts of suspicious activity
- Audit reporting and sign-offs
  - user activity
  - object creation
  - database configuration
  - entitlements
- Separation of duties – creation of policies vs. reporting on application of policies
- Trace users between applications, databases
- Fine grained-policies
- Sign-off and escalation procedures
- Integration with enterprise security systems (SIEM)



Ensure role separation, and use solutions that can deliver role-based reports, alerts, and controls.

-- Why Enterprise Database Security Strategy Has Become Critical, Forrester Research, Inc, July 13, 2011

Continuing to expand the Data Security portfolio

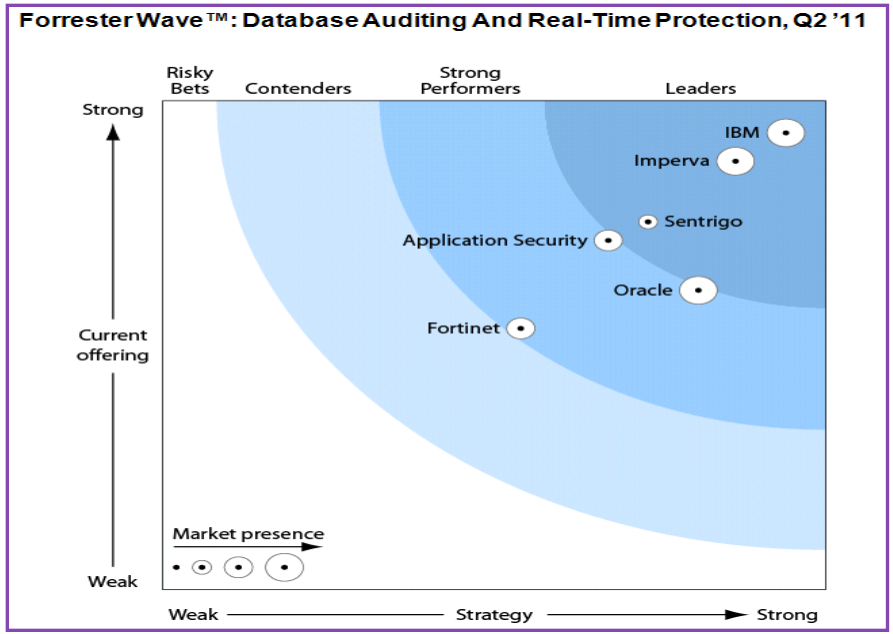
5 essentials for security and privacy

Security & Privacy

Discover Location of Sensitive Data	Mask data in non-production environments	Monitor database activity & assess vulnerabilities	Encrypt files in database environments	Redact unstructured data in documents
Automating the detection of sensitive data and enterprise data relationships	***Protect sensitive structured data in non-production environments (for dev, testing, offshore dev)***	***Provide essential safeguards to protect high value databases across heterogeneous environments***	***High performance data encryption***	***Protect stand-alone or embedded unstructured sensitive data in forms and documents***
Strengths: ✓ *Discover hidden data relationships to define business groupings of data* ✓ *Automate detection of sensitive data* ✓ *Reverse engineer transformation logic and prototype data consolidation rules*	*Strengths:* ✓ *Best practice for protecting sensitive data and supporting the testing process* ✓ *Mask information in 1 or many places using realistic values* ✓ *Reduce impact of internal and external data breaches*	*Strengths:* ✓ *Continuous, real-time database access and activity monitoring* ✓ *Policy-based controls to detect unauthorized or suspicious activity* ✓ *Vulnerability assessment, change auditing & blocking*	*Strengths:* ✓ *Encrypt files with minimal application impact* ✓ *Separation of duties for role efficiency – DBA vs IT Security* ✓ *Unified policy and key management for central administration*	*Strengths:* ✓ *Support redaction of textual, graphical, and form based data* ✓ *Increase efficiency via automation and reduce cost of manual redaction* ✓ *Control the data viewed by each user with policy rules*
InfoSphere Discovery & InfoSphere Guardium	**InfoSphere Optim Data Masking**	**InfoSphere Guardium DAM & VA Solution**	**InfoSphere Guardium Encryption Expert**	**InfoSphere Guardium Data Redaction**

Satisfy compliance and regulatory mandates

InfoSphere Guardium continues to demonstrate its leadership …



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.

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 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

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

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

Success: *Leading global household goods manufacturer protects the privacy of HR data within non-production systems*

Challenge

- This leading household goods manufacturer needed to **consolidate multiple worldwide instances** of the SAP Human Capital Management application
- As they created their testing environment, the client wanted to "de-identify" their SAP HCM data so that developers were not using **confidential employee HR data in their test environments**

Solution

- **IBM InfoSphere Optim Data Masking Solution for SAP Applications**

Business Benefits

- **Reduced time** to manually code the data scrambling routines
- **Implemented data masking solution**, as part of overall support data governance strategy
- **Protected confidential employee information** within the testing and development environments, ensuring privacy of HR and payroll information
- Deployed data masking solution **quickly and efficiently**, using both out-of-box definitions as well as custom de-identification routines

IBM InfoSphere Optim Data Masking Solution

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

Personal identifiable information is masked with realistic but fictional data for testing & development purposes.

Requirements

- Protect confidential data used in test, training & development systems
- Implement proven data masking techniques
- Support compliance with privacy regulations
- Solution supports custom & packaged ERP applications

Benefits

- Protect sensitive information from misuse and fraud
- Prevent data breaches and associated fines
- Achieve better data governance

Success: *Large insurance organization meets PCI DSS compliance requirements*

Challenge

- **Meet compliance requirements for PCI DSS** (Payment Card Industry Data Security Standard) for content management of historical documents and forms
- **Diverse groups need access to different information** in documents which contain personal health information (PHI) and confidential financial information (credit card numbers)
- **Replace current** cumbersome, lengthy **manual process** to redact forms and documents and minimize risk

Solution

- **IBM InfoSphere Guardium Data Redaction**

Business Benefits

- Boost time-to-value with quick implementation and high accuracy rates for redaction candidates
  - **97% accuracy**
- **Satisfy compliance requirements** in a timely manner
- **Increase efficiency and minimize risk of omissions** with automated identification and redaction of sensitive data

We are thoroughly impressed with IBM Optim Data Redaction, its capabilities and accuracy rates. This technology is helping us comply with PCIDSS (Payment Card Industry Data Security Standard) requirements for historical content management of documents and forms.

CSF International – Financial software provider

Challenge

- Satisfy the Payment Card Industry Data Security Standard (PCI DSS)
- Ensure that no device or system retains cardholder data
- Grow in new overseas markets to beat the competition and increase revenues
- Overcome the challenges of column level encryption including slow performance and difficult implementation

Solution

- **IBM InfoSphere Guardium Encryption Expert**
- **IBM Informix Dynamic Server**

Business Benefits

- Ensure compliance with Payment Card Industry Data Security Standard (PCI DSS)
- Simplify administration of security policies
- Use file level encryption to meet compliance regulations without affecting performance
- 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

Success: *Leading technology company simplifies enterprise security*

Challenge

- Improve database security for SOX, PCI & SAS70
  - Environment: Oracle & SQL Server on Windows, Linux; Oracle E-Business, JD Edwards, Hyperion plus in-house applications
- Simplify & automate compliance controls
  - Previous solution consisted of traces & auditing with in-house scripts, which impacted DBA resources, and lead to massive data volumes, supportability issues and SOD issues

Solution

- **IBM InfoSphere Guardium**

Business Benefits

- **Enterprise-class scalability**, deployed to 300 DB servers in 10 data centers in 12 weeks (deployed to additional 725 database servers in phase 2)
- Addressed critical needs for automated compliance reporting; real-time alerting; and centralized cross-DBMS policies
- Closed-loop change control with Remedy integration

The Guardium architecture offers a noninvasive, network-based, database-independent platform for continuously monitoring and analyzing database traffic in real time to help immediately identify unauthorized or suspicious activities.

IBM is your trusted partner …

Know how to ensure your success

Successfully implemented 1000s of client projects

Deliver value by understanding the big picture

Security across mainframes, desktops, networks, handheld devices

Help you to choose

Create the right solution for you

Expertise to meet your industry needs

Tailor solutions to meet your industry challenges

Ensure success by execution

Manage security for 400,000 IBM employees, 9B events/ day for clients

Client success stories to demonstrate results

Provided IT Security for 30+ yrs, 200 client references

Leverage our skills to meet your goals

1000s of researchers and SMEs

Partnership with a huge ecosystem

Large business partner community

Delivering solutions that enable enterprises to be Secure by Design.