IBM Security – Data Security

Yasser Abdalla, Sr. SW Specialist
My IBM home page : www.ibm.com/myrep/yasser_abdalla

© 2013 IBM Corporation
Customer Challenges  
*Data Security*

**Helping to prevent data breaches**  
- Mitigate internal and external threats across production and non-production environment.  
- Help to prevent disclosure or loss of sensitive data

**Maintaining the integrity of sensitive data**  
- Help to prevent unauthorized changes to data or structures

**Reducing the cost of compliance**  
- Automate and centralize controls
# Solving Customer Challenges

## Data Security

### Recent Breaches

<table>
<thead>
<tr>
<th>Company</th>
<th>Breach Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Heartland Payment Systems</td>
<td>100M credit cards stolen</td>
</tr>
<tr>
<td>Citi</td>
<td>200K+ account records stolen</td>
</tr>
<tr>
<td>Epsilon</td>
<td>92% of compromised records originate in DB servers</td>
</tr>
<tr>
<td>SK Telecom</td>
<td>Customer data of 2.5K brands lost</td>
</tr>
<tr>
<td></td>
<td>35M on-line accounts stolen</td>
</tr>
</tbody>
</table>

### Client Successes

<table>
<thead>
<tr>
<th>Company</th>
<th>Success Details</th>
</tr>
</thead>
</table>
| Tax authority of a major country | Help prevent data breaches
|                          | Tax authority detects inappropriate activity by privileged users with better controls to help prevent data breaches |
| Large Insurance Firm     | Maintain integrity of sensitive data                                             |
|                          | Insurance firm implemented privileged user Monitoring and change reconciliation; discovered unauthorized DBA activity |
| Global Financial Services Firm | Reduce the cost of compliance                                                  |
|                          | Global financial services firm subject to SOX reduced their operational costs to address compliance |
| Links Hospital           | Address regulatory mandates for privacy                                        |
|                          | Automatic encryption of data ensures protection that meets or exceeds regulatory standards at minimal cost |
Solutions for a Holistic Approach to Data Security and Compliance

**Understand and Define Sensitive Data**
Understand where data resides, how it's related and how to define the policies & metrics to protect data.

**Monitor and Audit**
Monitor transactions to enforce policies and capture a detailed audit trail.

**Assess Vulnerabilities**
Detect vulnerabilities to help harden sensitive repositories.

**Help Prevent Unauthorized Database Activities**
Block transactions that violate policy.

**Encrypt Data**
Encrypt structured and unstructured sensitive data to protect against unauthorized reading.

**Help Protect Sensitive Data in non-Production Databases**
De-identify sensitive data with data masking.

**Help Protect Unstructured Data**
Redact sensitive data in documents and forms.

**Manage Access**
Manage privileges and authenticate users to limit data access.
Challenge 1: Help Prevent Data Breaches

- Developers stealing data?
  - Copy of production data used for development

- Databases misconfigured?
  - Provides hackers with easy access

- Privileged Users viewing sensitive data?
  - Can easily bypass native logging based solutions

- Authorized user committing fraud?
  - Lack of detailed monitoring enables them to escape detection

- Monitor transactions without requiring changes to databases or applications
- Create realistic test sets while masking sensitive data values
- Encrypt regulated data to help prevent loss - particularly via theft of backups and media
- Redact stand-alone or embedded unstructured sensitive data in forms and documents
Challenge 2: Maintaining the Integrity of Sensitive Data

Privileged Users or outsourced personnel making unauthorized changes?
Most organizations have no control over DBA actions, and no means of effectively monitoring them.

Users bypassing application controls?
Credentials for enterprise applications often become well known; most organizations have no way of detecting or blocking application bypass.

Compare all transactions to policy and block violations in real-time.
Challenge 3: Reduce the Cost of Compliance

Can the audit data required by compliance mandates be easily assembled? 
Help protect centralized aggregation of audit data enterprise-wide, combined with comprehensive reporting capabilities simplify audit preparation

Are all policy violations detected and remediated? 
Demonstrate violations are investigated and closed using workflow automation to route incident data to oversight teams for sign-off

Is encryption deployed as required by regulatory mandates? 
Automate and centralize management of keys to simplify implementation of encryption

Automate and centralize controls to streamline compliance validation
Organizations Need a Comprehensive Enterprise-wide Approach to Data Security and Compliance

**Assess vulnerabilities**
- Automate detection of sensitive data and enterprise data relationships
  - Capabilities:
    - Discover database instances
    - Automate detection of sensitive data
    - Automate responsive actions
- Automate database vulnerability and configuration change detection
  - Capabilities:
    - Automated vulnerability assessment and remediation suggestions
    - Change auditing

**Monitor database activity**
- Provide essential safeguards to protect high value databases across heterogeneous environments
  - Capabilities:
    - Continuous, real-time database activity monitoring
    - Comprehensive audit trail
    - Policy-based controls to detect unauthorized or suspicious activity

**Help protect sensitive data**
- Help protect data – in both production & non-production, both structured & unstructured - from unauthorized use
  - Capabilities:
    - Mask information using realistic values
    - Automate key management process
    - Database encryption
    - Redact data in documents and forms

**Manage access**
- Manage and enforce privileges enterprise-wide
  - Capabilities:
    - Centralize and automate collection of entitlement information
    - Assess privileges granted directly and indirectly

---

**Infosphere Guardium Data Finder**
- Discover database instances
- Automate detection of sensitive data
- Automate responsive actions

**Infosphere Data Discovery**
- Automate database vulnerability and configuration change detection
- Capabilities:
  - Automated vulnerability assessment and remediation suggestions
  - Change auditing

**Infosphere Guardium Data Vulnerability Assessment**
- Automate detection of sensitive data
- Automate responsive actions

**Infosphere Guardium Data Activity Monitoring**
- Provide essential safeguards to protect high value databases across heterogeneous environments
- Capabilities:
  - Continuous, real-time database activity monitoring
  - Comprehensive audit trail
  - Policy-based controls to detect unauthorized or suspicious activity

**Infosphere Guardium Data Encryption**
- Help protect data – in both production & non-production, both structured & unstructured - from unauthorized use
- Capabilities:
  - Mask information using realistic values
  - Automate key management process
  - Database encryption
  - Redact data in documents and forms

**IBM Key Lifecycle Manager**
- Manage and enforce privileges enterprise-wide
- Capabilities:
  - Centralize and automate collection of entitlement information
  - Assess privileges granted directly and indirectly

**Infosphere Optim Data Masking**
- Help protect data – in both production & non-production, both structured & unstructured - from unauthorized use
- Capabilities:
  - Mask information using realistic values
  - Automate key management process
  - Database encryption
  - Redact data in documents and forms

**Infosphere Guardium Data Redaction**
- Help protect data – in both production & non-production, both structured & unstructured - from unauthorized use
- Capabilities:
  - Mask information using realistic values
  - Automate key management process
  - Database encryption
  - Redact data in documents and forms
Helping Organizations Progress in Their Security Maturity

<table>
<thead>
<tr>
<th>Security Intelligence</th>
<th>People</th>
<th>Data</th>
<th>Applications</th>
<th>Infrastructure</th>
<th>Security Intelligence</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Optimized</strong></td>
<td>Role based analytics&lt;br&gt;Identity governance&lt;br&gt;Privileged user controls</td>
<td><strong>Data flow analytics</strong>&lt;br&gt;<strong>Data governance</strong></td>
<td>Secure app engineering processes&lt;br&gt;Fraud detection</td>
<td>Advanced network monitoring&lt;br&gt;Forensics / data mining&lt;br&gt;Securing systems</td>
<td>Advanced threat detection&lt;br&gt;Network anomaly detection&lt;br&gt;Predictive risk management</td>
</tr>
<tr>
<td><strong>Proficient</strong></td>
<td>User provisioning&lt;br&gt;Access mgmt&lt;br&gt;Strong authentication</td>
<td><strong>Access monitoring</strong>&lt;br&gt;<strong>Data loss prevention</strong></td>
<td>Application firewall&lt;br&gt;Source code scanning</td>
<td>Virtualization security&lt;br&gt;Asset mgmt&lt;br&gt;Endpoint / network security management</td>
<td>Real-time event correlation&lt;br&gt;Network forensics</td>
</tr>
<tr>
<td><strong>Basic</strong></td>
<td>Centralized directory</td>
<td><strong>Encryption</strong>&lt;br&gt;<strong>Access control</strong></td>
<td>Application scanning</td>
<td>Perimeter security&lt;br&gt;Anti-virus</td>
<td>Log management&lt;br&gt;Compliance reporting</td>
</tr>
</tbody>
</table>
IBM’s security product and service portfolio

<table>
<thead>
<tr>
<th>Security Intelligence, Analytics and GRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>QRadar SIEM</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IT Infrastructure – Operational Security Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>People</td>
</tr>
<tr>
<td>Identity and Access Management Suite</td>
</tr>
<tr>
<td>Federated Identity Manager</td>
</tr>
<tr>
<td>Enterprise Single Sign-On</td>
</tr>
<tr>
<td>Identity Assessment, Deployment and Hosting Services</td>
</tr>
<tr>
<td>Data</td>
</tr>
<tr>
<td>InfoSphere Guardium Database Security</td>
</tr>
<tr>
<td>InfoSphere Optim Data Masking</td>
</tr>
<tr>
<td>Key Lifecycle Manager</td>
</tr>
<tr>
<td>Data Security Assessment Service</td>
</tr>
<tr>
<td>Encryption and DLP Deployment</td>
</tr>
<tr>
<td>Applications</td>
</tr>
<tr>
<td>AppScan Enterprise, Standard and Source</td>
</tr>
<tr>
<td>DataPower Security Gateway</td>
</tr>
<tr>
<td>Security Policy Manager</td>
</tr>
<tr>
<td>Application Assessment Service</td>
</tr>
<tr>
<td>AppScan OnDemand - SaaS</td>
</tr>
<tr>
<td>Network</td>
</tr>
<tr>
<td>Network Intrusion Prevention</td>
</tr>
<tr>
<td>SiteProtector Management System</td>
</tr>
<tr>
<td>QRadar Anomaly Detection</td>
</tr>
<tr>
<td>Managed Firewall, UTM, and Intrusion Prevention Services</td>
</tr>
<tr>
<td>Endpoint</td>
</tr>
<tr>
<td>Endpoint Manager (BigFix)</td>
</tr>
<tr>
<td>Virtualization and Server Security</td>
</tr>
<tr>
<td>Mainframe Security (zSecure, RACF)</td>
</tr>
<tr>
<td>Penetration Testing Services</td>
</tr>
<tr>
<td>Mobile Device Management</td>
</tr>
</tbody>
</table>

IBM Security Portfolio

<table>
<thead>
<tr>
<th>Enterprise Governance, Risk and Compliance Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRC Platform (OpenPages)</td>
</tr>
</tbody>
</table>
# Data Security Product Line up

<table>
<thead>
<tr>
<th>Product</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM Infosphere Guardium Database Activity Monitoring</td>
<td>Provides a simple, robust solution that helps prevent leakage of sensitive data from databases and files, maintaining the integrity of information in the data center and automating compliance controls across heterogeneous environments</td>
</tr>
<tr>
<td>IBM Infosphere Guardium Vulnerability Assessment</td>
<td>Provides the capability to automate the detection of database vulnerabilities, and suggest prioritized remedial actions across heterogenous infrastructures</td>
</tr>
<tr>
<td>IBM Infosphere Guardium Data Redaction</td>
<td>Helps protect sensitive data in documents and forms from unintentional disclosure, detecting &amp; removing the data from the document version openly shared</td>
</tr>
<tr>
<td>IBM Infosphere Guardium Data Encryption</td>
<td>Provides a single, manageable and scalable solution to encrypt enterprise data without sacrificing application performance or creating key management complexity</td>
</tr>
<tr>
<td>IBM Infosphere Optim Data Masking</td>
<td>Provides an extensive set of data masking techniques to de-identify confidential information to help protect privacy and support compliance initiatives</td>
</tr>
<tr>
<td>IBM Key Lifecycle Manager</td>
<td>Helps IT organizations better manage the encryption key life cycle by enabling them to centralize and strengthen key management processes by leveraging industry standard KMIP (Key Management Interoperability Protocol)</td>
</tr>
<tr>
<td>IBM Infosphere Discovery</td>
<td>Helps identify and document what data you have, where it is located and how it’s linked across systems by intelligently capturing relationships and determining applied transformations and business rules</td>
</tr>
</tbody>
</table>
Why IBM Security: Breadth, deep expertise, integration

**Leadership**
- More Global 1000 organizations use InfoSphere Guardium to help secure their critical enterprise data than any other technology provider
- Forrester’s TEI study demonstrates a 239% ROI for InfoSphere Guardium Database Activity Monitor **
- Forrester’s TEI Study finds organizations realize a 20% reduction in the time required to complete audits, about $50,000/year, using InfoSphere Optim Data Masking **
- “IBM continues to demonstrate its leadership in supporting very large heterogeneous environments, delivering high performance and scalability, simplifying administration and performing real time database protection” – Forrester *

**Integration**
- Integrates with other security products including the zSecure suite and IBM QRadar solution for Security intelligence

**Expertise**
- Backed by X-Force, one of the largest security research teams
- 9 security research centers combined with 9 security operations centers around the world

* Forrester Wave: Database Auditing And Real-Time Protection, Q2’11 (Forrester)
** Forrester Consulting: The Total Economic Impact Of Guardium Database Security, Monitoring and Auditing, 2008
© 2013 IBM Corporation
THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.