Database Attacks Exposed
What we’ll discuss in this session

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

% of Compromised Records

<table>
<thead>
<tr>
<th>Year</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009</td>
<td>75%</td>
</tr>
<tr>
<td>2010</td>
<td>92%</td>
</tr>
</tbody>
</table>


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

- Database servers contain your most valuable information
  - Financial records
  - Credit card and other account records
  - Patient records
  - Personally identifiable information
  - Customer data
- High volumes data
- Structured for easy to access
Perimeter defenses no longer sufficient

“A fortress mentality will not work in cyber. We cannot retreat behind a Maginot Line of firewalls.”

-- William J. Lynn III, U.S. Deputy Defense Secretary
Database danger from within

 “Organizations overlook the most imminent threat to their databases: authorized users.” (Dark Reading)

 Most organizations (62%) cannot prevent super users from reading or tampering with sensitive information … most are unable to even detect such incidents … only 1 out of 4 believe their data assets are securely configured (Independent Oracle User Group).

The Enterprise Patching Issue

• Nearly half of companies lack a format patch management process
• 62% typically take 3 months or more to apply Critical Patch Updates (IOUG)
• Only 18% measure patch success via configuration scanning
• "The least mature areas of patching seem to correlate almost directly with the fastest-growing areas of attacks, such as … database servers [and] business application servers."

"Patch management is one of the most fundamental functions of IT departments, yet in our research we discovered it remains one of the biggest pain points for many organizations."

Rich Mogull, Securosis

http://www.darkreading.com/database_security
http://www.securosis.com/projectquant
Compromises take days or more to discover in 79% of cases; and weeks or more to contain in over in 53% of cases

Time span of events by percent of breaches

<table>
<thead>
<tr>
<th>Point of Entry to Compromise</th>
<th>Minutes</th>
<th>Hours</th>
<th>Days</th>
<th>Weeks</th>
<th>Months</th>
<th>Years/Never</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>33%</td>
<td>14%</td>
<td>44%</td>
<td>5%</td>
<td>4%</td>
<td>&lt;1%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Compromise to Discovery</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&lt;1%</td>
<td>4%</td>
<td>17%</td>
<td>38%</td>
<td>36%</td>
<td>5%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Discovery to Containment</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&lt;1%</td>
<td>11%</td>
<td>23%</td>
<td>49%</td>
<td>15%</td>
<td>2%</td>
</tr>
</tbody>
</table>
Typical home-grown solutions are costly and ineffective

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

Native Database Logging

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

- No separation of duties; DBA run the process
- Performance impact of native logging on the DBMS
- Limited scope of logging data
- Not real-time
- Significant labor cost to review data and maintain process
- Another data store to secure and manage
- Manual remediation is error prone and costly
- Poor audit trail
- Inconsistent policies across systems and business units
- Lack of DBMS expertise
Real time database monitoring and protection with InfoSphere Guardium

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

- Cross-DBMS solution
- Granular, real-time policies & auditing
  - Who, what, when, how
- Automated compliance reporting, sign-offs and escalations (financial regulations, PCI DSS, data privacy regulations, etc.)
Scalable architecture supports application-specific and enterprise-wide deployments
Addressing the full database security lifecycle

**Monitor & Enforce**
- Prevent cyberattacks
- Monitor & block privileged users
- Detect application-layer fraud
- Enforce change controls
- Real-time alerts
- Control firewall IDs
- SIEM integration

**Audit & Report**
- Automated & centralized controls
- Cross-DBMS audit repository
- Preconfigured policies/reports
- No database changes
- Minimal performance impact
- Sign-off management
- Entitlement reporting

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

**Assess & Harden**
- Assess static and behavioral database vulnerabilities
- Configuration auditing
- Preconfigured tests based on best practices standards (STIG, CIS, CVE)
Find uncataloged databases and identify sensitive data

- Crawls the network to find uncataloged instances
- Four algorithms to identify sensitive data in databases
- Policy-based responsive actions
  - Alerts
  - Add to group of sensitive objects
Harden databases by identifying unpatched and misconfigured systems
## Eliminate inappropriate privileges

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

- Provides a simple means of aggregating and understanding entitlement information
  - Scans and collects information on a scheduled basis, including group and role information

- Out-of-the-box reports for common views

- Report writer for custom views

- Eliminates resource intensive and error prone processes of manually examining each database and stepping through roles

### Example Reports

<table>
<thead>
<tr>
<th>Accounts with system privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>All system and admin privileges (by user / role)</td>
</tr>
<tr>
<td>Object privileges by user</td>
</tr>
<tr>
<td>Roles granted (user and roles)</td>
</tr>
<tr>
<td>Privilege grants</td>
</tr>
<tr>
<td>Execute privileges by procedure</td>
</tr>
</tbody>
</table>
Cross-platform policies and auditing for enterprise-wide deployment

- Unified cross-platform policies easily defined
- Responsive actions defined within policies
- Single audit repository enables enterprise-wide compliance reporting and analytics
A simple policy example: Preventing application bypass

- Application Server: 10.10.9.244
- Database Server: 10.10.9.56

Sample Alert

```
Subject: (c1) SQLGUARD ALERT Alert based on rule ID 20267 [non-App Source AppUser Connection]
Category: security Classification: Breach Severity: MED
Rule # 20267 [non-App Source AppUser Connection]
Application User Name: Source Program: DBC TNS CLIENT Authorization Code: 1 Request Type: SQL_LANG Last Error:
SQL: select * from EmployeeTable
```
Prevent policy violations in real-time (blocking)

- No database changes
- No application changes
- No network changes
- Without the performance or availability risks of an in-line database firewall
Identify inappropriate use by authorized users

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

<table>
<thead>
<tr>
<th>DB User Name</th>
<th>Sql</th>
<th>Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>STEVE</td>
<td><code>select * from ar.creditcard where i&gt;=? and i&lt;=? 4</code></td>
<td></td>
</tr>
<tr>
<td>HARRY</td>
<td><code>select * from ar.creditcard where i&lt;=?</code></td>
<td>4</td>
</tr>
<tr>
<td>JOE</td>
<td><code>select * from ar.creditcard where i&lt;=?</code></td>
<td>99</td>
</tr>
</tbody>
</table>

Is this normal?

What did he see?
Automate oversight processes to ensure compliance and reduce operational costs

- Easily create custom processes by specifying unique combination of workflow steps, actions and users
  - Use case
    Different oversight processes for financial servers than PCI servers

- Supports automated execution of oversight processes on a report line item basis, maximizing efficiency without sacrificing security
  - Use case
    Daily exception report contains 4 items I know about and have resolved, but one that needs detailed investigation. Send 3 on for sign-off; hold one
InfoSphere Guardium allows you to protect your most valuable information

Continuously monitor access to high-value databases to:

1. Prevent data breaches
   Mitigate external and internal threats

2. Ensure the integrity of sensitive data
   Prevent unauthorized changes to sensitive data or structures

3. Reduce cost of compliance
   Automate and centralize controls
   1. Across PCI DSS, data privacy regulations, HIPAA/HITECH, …
   2. Across databases and applications
   Simplify processes
DAM Provides a Simple Means of Centralizing and Automating Controls

- Discovering and applying controls to all sensitive data
- Controlling who accesses and modifies what data, from where, and when
- Managing exposure to misuse of credentials, privileges, etc.
- Ensuring sensitive data stores are appropriately configured
- Standardizing, automating and streamlining the review and remediation of policy violations, as well compliance validation activities
- Without compromising separation of duties or performance
Can You Afford a DAM Solution?

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

- **Who:** World’s largest dedicated security company
- **Need:** Safeguard millions of PCI transactions
  - Maintain strict SLAs with ISP customers (Comcast, COX, etc.)
  - Automate PCI controls
- **Environment:** Guardium deployed in less than 48 hours
  - Multiple data centers; clustered databases
  - Integrated with ArcSight SIEM
  - Expanding coverage to SAP systems for SOX
- **Previous Solution:** Central database audit repository with native DBMS logs
  - Massive data volumes; performance & reliability issues; SOD issues
- **Results:**
  - “McAfee needed a solution with continuous real-time visibility into all sensitive cardholder data – in order to quickly spot unauthorized activity and comply with PCI-DSS – but given our significant transaction volumes, performance and reliability considerations were crucial.”
  - “We were initially using a database auditing solution that collected information from native DBMS logs and stored it in an audit repository, but granular logging significantly impacted our database servers and the audit repository was simply unable to handle the massive transaction volume generated by our McAfee.com environment.”
Implementing automated and centralized controls yields global manufacturer 239% ROI

**Challenge**

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

**Business Benefits**

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

Commissioned Forrester Consulting Case Study
Simplifying enterprise security for Dell

**Challenge**

- **Who**: Leading global supplier of PCs and technology products. $61B in revenue; 257th in Global Fortune 500
- **Need**:
  - Improve database security for SOX, PCI and SAS70
  - Simplify and automate compliance controls
- **Environment**:
  - Oracle and SQL Server on Windows, Linux; Oracle RAC, SQL Server clusters
  - Oracle EBS, JDE, Hyperion plus in-house applications
- **Previous Solution**:
  - Native logging (MS) or auditing (Oracle) with in-house scripts
  - Supportability issues; DBA time required; massive data volumes; SOD issues

**Business Benefits**

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

**Solution**

- **InfoSphere Guardium Deployment**:
  - Phase 1: Deployed to 300 DB servers in 10 data centers (in 12 weeks)
  - Phase 2: Deployed to additional 725 database servers
Chosen by over 500 leading organizations worldwide

- 5 of the top 5 global banks
- 2 of the top 3 global retailers
- 5 of the top 6 global insurers
- The most recognized name in PCs
- 4 of the top 4 managed healthcare providers globally
- Top government agencies
- 8 of the top 10 telcos worldwide
InfoSphere Guardium continues to demonstrate its leadership …

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

<table>
<thead>
<tr>
<th>Awarded highest score in overall “Market Presence”</th>
<th>The Evaluation Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awarded highest score in overall “Strategy”</td>
<td>6 of the top vendors evaluated</td>
</tr>
<tr>
<td>Awarded highest score in evaluation of “Current Offering”</td>
<td>Examined past research</td>
</tr>
<tr>
<td>Achieved highest score possible in 8 out of 16 high-level scored categories</td>
<td>Customer reference calls</td>
</tr>
<tr>
<td>Achieved the top ranking in 7 high-level categories; tied for top ranking in 1 category</td>
<td>Conducted user needs assessments</td>
</tr>
<tr>
<td>Evaluation based on v7, v8 introduced weeks after cutoff</td>
<td>Conducted vendor and expert interviews</td>
</tr>
<tr>
<td></td>
<td>Examined product demos</td>
</tr>
<tr>
<td></td>
<td>Conducted lab evaluations</td>
</tr>
<tr>
<td></td>
<td>147 evaluation criteria</td>
</tr>
</tbody>
</table>
IBM’s acquisition of Guardium in 2009 changed everything, making IBM one of the leading players.

“IBM continues to focus on innovation....”

“IBM InfoSphere Guardium continues to demonstrate its leadership in supporting very large heterogeneous environments, delivering high performance and scalability, simplifying administration and performing real-time database protection”

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

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

Forrester Wave™: Database Auditing And Real-Time Protection, Q2 2011, May 6, 2011
Mastering information across the Information Supply Chain

- **Manage**: Transactional & Collaborative Applications, Data, Content, Streaming Information, External Information Sources
- **Integrate**: Master Data, Integrate & Cleanse, Data Warehouses
- **Analyze**: Content Analytics, Big Data, Cubes, Streams, Business Analytics Applications
- **Govern**: Quality, Lifecycle, Security & Privacy, Standards

**Trust**ed  ◆ **Relevant**  ◆ **Governed**
Summary

- In the current environment, a means for securing high-value databases and validating compliance is a necessity

- Traditional log management, SIEM and DLP solutions are insufficient to secure sensitive databases
  - No real-time monitoring at data level to detect unauthorized activities
  - Native logging/auditing require database changes and impact performance
  - No knowledge of DBMS commands, vulnerabilities and structures
  - Inability to detect fraud at application layer

- InfoSphere Guardium is the most widely-deployed solution, with ongoing feedback from the most demanding data center environments worldwide
  - Scalable enterprise architecture
  - Broad heterogeneous support
  - Complete visibility and granular control
  - Deep automation to reduce workload and total cost of operations
  - Holistic approach to security and compliance
Broad array of additional resources available

- Analyst reports
  - Forrester Wave (link also located on top right corner of Guardium page)
  - Gartner: 10 Database Activities You Need to Monitor
  - Forrester: Your Enterprise Database Security Strategy
  - Forrester: Look Beyond Database Auditing to Improve Security, Audit Visibility and Real-Time Protection

- Technical on-demand webinars
  - Vulnerability Assessment, Protecting Against Top 5 Threats
  - Verizon: Data Breach Investigations Report
  - Forrester: Best Practices for DB Security and Compliance

- Chapter downloads of database security texts
  - Implementing Database Security and Auditing
  - HOWTO Secure and Audit Oracle 10g and 11g

Go to ibm.com and search for InfoSphere Guardium; look for the “Library” tab in the top left corner.
**Broadest platform support in the industry**

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