Security

- User Management
- Access Control
- Data Protection
- Monitoring

Key Drivers for Data Security

Regulatory Compliance

- Sarbanes-Oxley (SOX),
- Foreign Exchange Instruments and Exchange Law (J-SOX)
- EU Privacy Directives, CA SB 1386…
- Payment Card Industry (PCI)
- Adequate IT controls, COSO, COBIT
- Separation of duty, Proof of compliance, Risk Assessment and Monitoring

Insider Threats

- Large percentage of threats go undetected
- Outsourcing and off-shoring trend
- Customers want to monitor insider/DBA
Oracle Database Security Products

**User Management**
- Oracle Identity Management
- Enterprise User Security

**Access Control**
- Oracle Database Vault
- Oracle Label Security

**Monitoring**
- Oracle Audit Vault
- EM Configuration Pack

**Data Protection**
- Oracle Advanced Security
- Oracle Secure Backup

---

Oracle Database 11g

**Enterprise User Security**

- User Management for Compliance
  - Centralized User Management
  - Consolidate database accounts with shared database schemas
  - Centrally managed DBAs
  - Validated with Oracle Virtual Directory
- Enterprise Strong Authentication
  - Kerberos (MSFT, MIT)
  - PKI (x.509v3)
  - Password
  - SYSDBA Strong Authentication
- Database Enterprise Edition Feature
  - Requires Oracle Identity Management
  - Available since Oracle 8.1.6

---

Oracle Identity Management
Oracle Database Security Products

User Management
- Oracle Identity Management
- Enterprise User Security

Access Control
- Oracle Database Vault
- Oracle Label Security

Core Platform Security

Monitoring
- Oracle Audit Vault
- EM Configuration Pack

Data Protection
- Oracle Advanced Security
- Oracle Secure Backup

Oracle Label Security

Manageability

- Policy based model
- Multiple policies supported
  - ACME, HR, Legal
- Policies are umbrellas applying to one or more tables, schemas, users
- Web based management
  - Integrated with Oracle Identity Management

<table>
<thead>
<tr>
<th>Level</th>
<th>Short Name</th>
<th>Numeric Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONFIDENTIAL</td>
<td>C</td>
<td>1000</td>
</tr>
<tr>
<td>SENSITIVE</td>
<td>S</td>
<td>2000</td>
</tr>
<tr>
<td>HIGHLY SENSITIVE</td>
<td>HSS</td>
<td>3000</td>
</tr>
</tbody>
</table>
Oracle Database Security Products

User Management
- Oracle Identity Management
- Enterprise User Security

Access Control
- Oracle Database Vault
- Oracle Label Security

Monitoring
- Oracle Audit Vault
- EM Configuration Pack

Data Protection
- Oracle Advanced Security
- Oracle Secure Backup

Core Platform Security

Oracle Advanced Security

Tablespace Encryption

- Define a new tablespace as ‘encrypted’
  - cannot convert existing, un-encrypted tablespaces
  - however, content can be moved into encrypted tablespaces
- Always salted for higher security
- Overcomes limitation of column-based TDE:
  - supports indexes other than b-tree
  - supports foreign keys
- No additional management overhead
  - integrated into TDE key management, same wallet used as for column based Transparent Data Encryption
- No storage overhead (!)
Oracle Advanced Security
Master key stored in HSM device

- Store the Master key in an external hardware device
- Master key never leaves the device
- Standard PKCS #11 API allows customers to choose from a wide range of HSM vendors
- Encryption and decryption done on the database server
- Simplifies key management in distributed environments (data guard, RAC)

Oracle Advanced Security
SECUREFILE LOB Encryption

- SECUREFILE LOB encryption
- All SECUREFILE LOBs in an encrypted column are encrypted
  - In-line (in table) and out-of-line (in tablespace) are both encrypted
  - BFILEs are not encrypted
  - Always salted for higher security
Oracle Database Security Products

User Management
- Oracle Identity Management
- Enterprise User Security

Access Control
- Oracle Database Vault
- Oracle Label Security

Monitoring
- Oracle Audit Vault
- EM Configuration Pack

Data Protection
- Oracle Advanced Security
- Oracle Secure Backup

Core Platform Security

Oracle Database 11g
Security Manageability

- Integrated with EM
- Label Security
- Virtual Private Database
- Application Context
- Enterprise Security Manager
- Transparent Data Encryption
11g Database Manageability

- Memory Management
- AWR Baselines
- Automatic SQL Tuning
- Advisors
- Upgrade Considerations

11g Database Manageability

Automatic Memory Management
Memory Management in 10g/11g

**11g Automatic Memory Management**
- `MEMORY_TARGET`
- `MEMORY_MAX_TARGET`
- Improves memory utilization
- Eases memory management

**10g Automatic Shared Memory Management (ASMM)**
- `SGA_TARGET`
- Key shared memory components tuned automatically
- Single parameter controls all shared memory

**10g Automatic PGA Memory Management**
- `PGA_AGGREGATE_TARGET`
- Various PGA sort areas tuned automatically
- Single parameter controls all PGA memory

**Automatic Memory Management in 11g**
- Unifies system (SGA) and process (PGA) memory management
- Dynamic parameters for all database memory:
  - `MEMORY_TARGET`
  - `MEMORY_MAX_TARGET`
- Automatically adapts to workload changes
- Maximizes memory utilization
- Available on:
  - Linux
  - Windows
  - Solaris
  - HPUX
  - AIX
Memory Target Benefits

- Balances dynamic memory needs of SGA and PGA
  - Previously either or both could end up undersized
  - PGA can grow but not to the detriment of SGA performance
  - Best-effort memory transfers
  - Tunable PGA can help relieve 4031 from SGA

- Built-in safety nets:
  - Decides victim components
  - Paced memory donation avoids thrashing
  - Run-away workload cannot starve resources
  - Component-specific settings still honored