“Leap Forward” with Oracle Identity Management


Leverage - Your Oracle Application investment

Extend - Its capabilities to solve common security problems, drive down costs and boost end user productivity

Automate - Costly and Time-Consuming User Management, User Access, Access Recertification and Reporting processes

Protect - Your Oracle Application “to the Core” with strong access controls, segregation of duties and data protection
Oracle IDM Drives Productivity!

**Annual Minutes Required for Identity**

- **Identity & Audit Tasks:**
  - User Administration
  - Password Reset
  - Internal Audit

**Annual Cost Comparison, Business-as-Usual vs. Oracle IDM**

- **Productivity**
- **User Satisfaction**
- **Identity & Audit Costs Down 55%**

$7.4M Savings over 4 Years
$3M Year-Over-Year Savings Year Once Fully Deployed!

Today’s Agenda

- Security + Compliance Issues Application Customers Face
- Solving Issues with Oracle Identity Management and Security
  - Automating User & Password Management
  - Simplifying Sign On & Centralizing Access Management
  - Streamline Governance, Risk and Compliance
- ‘Real World’ Case Studies
  - Oracle Application customers using Identity Management today?
Oracle Applications are a Great Foundation!
Overall Business Pressures

Ever-Changing Workforce
- How can I cost-effectively manage a mixed set of users?
- How can I develop an agile workforce to support changing business?

Governance & Compliance
- How can I keep pace with changing privacy laws & safety regulations?
- How can I gain greater control of processes, data, and approvals?

Globalization and Emerging Markets
- What is the best way to service an increasingly global workforce?
- How can I simplify complex processes across the organization?

Reduce Costs While Improving Service
- Where can I cut costs & improve efficiencies?
- How can I manage and improve workforce utilization?
**Issue #1: Managing Users and Entitlements**

1. **Creating** user accounts and granting fine-grained entitlements (Roles, Responsibilities) is manual and costly.

2. **Transfers** are hard to handle and removing excessive privileges doesn’t happen fast enough.

3. **Requesting** new user access is a manual effort that takes too long.

4. **Access approvals** are manual, email-driven, aren’t unique for the access request and aren’t auditable.

5. **Removing** user access and entitlements upon termination takes too long and has lots of spot issues.

**Issue #2: Access and Password Management**

1. We want to make access to applications easier by either using SSO or the user’s AD password.

2. Users forget their passwords, we need a way for them to reset it themselves.

3. We’d like to use SSO, but have to be sure we know who the user is and prevent fraud.

4. We’d like to expose our applications externally to all users over the web vs. VPN but don’t have confidence.

5. We need fine-grained access control of application data (at the UI and database levels).
Issue #3: Governance, Risk and Compliance

1. “Who has” and “Who had access to what?” and “Why?” reports are manual and sometimes impossible
2. Segregation of Duties (SoD) within the application is difficult to achieve even at a ‘detective’ level
3. Orphaned/ghost accounts are very hard detect and eliminate. There could be hundreds or thousands?
4. We can’t ensure the protection of our application’s database data and prove controls are working
5. Out of all these issues, “Periodic Access Reviews” are the most complex, costly and time-intensive task

What Application Customers Are Asking For...

- Business Users
  - Need User Accounts and Entitlements As Fast As Possible
  - Want Simplified Access To ALL Applications
  - Minimize or Synchronize the passwords

- IT Personnel
  - Needs Help Simplifying User Management For:
    - Employees
    - Customers
    - Partners
  - Want to workflow to automate manual processes
  - Need Tools To Manage IT Systems With Less Effort

- Information Security and Audit
  - Need To Understand Risk And What To Protect
  - Want to Protect Data From Compromise
  - Looking to Review User Access in less time
  - Need Reports For “Who Has (And Had) Access To What?”
We Can Fix These Issues Today

Extend.

Automate
- User & Responsibility
- Secure, Risk-Based Single Sign On
- Self Service Password Reset and Account Requests

Protect
- Web-Based Periodic Access Review
- Preventive Segregation of Duties Controls
- Strong Access Controls and Data Protection
“Securing, Automating and Auditing”

Oracle Applications

Get Productive!

Get Compliant!

HR-Driven User Mgmt
Automatically on-board, transfer and off-board users based on HR events

Role-Based Access
Automatically grant User rights and generate auditable approval workflows

Risk-Based SSO
Users access to apps on Day 1 using SSO and optional strong authentication that employs risk analytics

User Self Service
Web-based home page for requesting new access rights and changing passwords

Segregation of Duties
“Preventative and Detective” SoD ensure compliance and reports are generated for audit

Periodic Access Review
Web-Based, Interface used to schedule, delegate, track, complete and view reports for audit

Data Protection
“Edge to Core” security of application data ensures users only get access to what they need

Oracle IdM is “Certified and Ready”

Access Manager
Adaptive Access Manager
Identity Federation
Entitlement Server
Enterprise SSO Suite
Identity Manager
Role Manager
Internet Directory
Virtual Directory
Web Services Manager

In Progress In Progress In Progress In Progress

Out-of-The-Box Connectors Certified Interoperability

Get Productive!

Oracle Applications

Get Compliant!

HR-Driven User Mgmt
Automatically on-board, transfer and off-board users based on HR events

Role-Based Access
Automatically grant User rights and generate auditable approval workflows

Risk-Based SSO
Users access to apps on Day 1 using SSO and optional strong authentication that employs risk analytics

User Self Service
Web-based home page for requesting new access rights and changing passwords

Segregation of Duties
“Preventative and Detective” SoD ensure compliance and reports are generated for audit

Periodic Access Review
Web-Based, Interface used to schedule, delegate, track, complete and view reports for audit

Data Protection
“Edge to Core” security of application data ensures users only get access to what they need

Oracle IdM is “Certified and Ready”

Access Manager
Adaptive Access Manager
Identity Federation
Entitlement Server
Enterprise SSO Suite
Identity Manager
Role Manager
Internet Directory
Virtual Directory
Web Services Manager

In Progress In Progress In Progress In Progress

Out-of-The-Box Connectors Certified Interoperability
How Do We ‘Automate Security’?
Automated User and Responsibility Management

**Issue to Address**
- Creating user accounts and granting them the Entitlements they need is manual and costly.
- Transfers are hard to handle. Termination of unused privileges isn’t happening fast enough.
- Removing access and entitlements upon termination takes too long and has spot issues.
- Orphaned/ghost accounts are very hard to detect and eliminate. There could be thousands?

**Solution**
- Oracle Identity Manager
- Option: Oracle Role Manager

Automatic User and Entitlement Mgmt

‘Single Global Instance’ of All Users

**HR & Biz Applications**
- Oracle Identity Manager
- On-board, Transfer, Update, Off-board Users
- Add and Remove Application Entitlements
- Password Update and Synchronization
- ‘Certified’ Apps Integration

**Other Sources**
- Flat Files
- Databases
- Directories

Oracle Database

User Account and Entitlements Created/Modified

User Account and Entitlements

1. Pull lists of Who is in each system
2. Periodically Check for Rogue Identities
3. Remove Identities and/or Entitlements
Automatic User and Entitlement Mgmt
‘Single Global Instance’ of All Users

Manage Roles, Approvers & Orgs
Oracle Role Manager

MAPS:
Business Roles TO
IT/System Roles TO
Entitlements TO
Approvers

Oracle Role Manager
Role Mining
Role Management
Organization and Hierarchy Management
“Who is the Approver?”

HR and Other Applications
Oracle Identity Manager
Account Reconciliation
Account Provisioning
Entitlement Management
Approval Workflows

Go To Identity Manager’s Self Service and Approve Chris’ Request?

Leverage Extend Automate Protect
Manage Roles, Approvers & Orgs
Oracle Role Manager

IDM Impact on User Management

Key Takeaways
- **Then:** 10 business days for account creation/modification and sometimes termination!
- **Now:** Under 1 day (could be real-time without approvals)
- **Results:**
  - Improved Customer Service
  - Reduced Cost

Business Days Required for New Account Creation

- **Before Oracle IDM Implementation:**
  - 0 days
- **Today:**
  - Under 1 day
‘Automated Security’ for Oracle Applications

Secure, Risk-Based, Single Sign On

We want to make access to Apps easier by either using SSO or the user's AD password.

We'd like to use SSO, but have to be sure we know who the user is and prevent fraud.

We'd like to expose more functionality externally but want higher levels of security.

Solution

Option #1: Oracle Directory Services

Option #2: Other Access Suite Components

Option #3: Enterprise SSO Suite
Enable Single Sign-On
Oracle Access Manager (with/without OSSO)

- Extranet & Intranet SSO
- Self Service Registration
- Audit User Access
- Optional “Bolt-On”
- Stronger Authentication

Corporate Directory

Automating User Sign-On
‘Bolt-On’ Fraud Prevention and Strong AuthN

Oracle Adaptive Access Manager

Suppliers

Employees

Customers

Prevents: Phishing, Pharming, Trojans, Key logging, Proxy Attacks, Insider threats

‘Automated Security’ for Oracle Applications

Automate

Secure, Risk-Based Single Sign On

Self Service Password Reset and Account Requests

Automate User & Responsibility

Computed Risk Score
**Self Service Password Reset & Account Requests**

### Issue to Address
- Requesting new entitlements on each system is a manual effort that takes too long.
- Approval for new entitlements is manual and not auditable.
- App users forget their passwords, and there is no way for them to reset it themselves.

### Solution
- Oracle Identity Manager

**Web Based, User Self Service**

**Oracle Identity Manager**

Add Responsibilities

- Leverage
- Extend
- Automate
- Protect
Options for Obtaining Responsibilities

- Web-Based Approval Policy Creation & Modification
- Example ‘Manager and IT Owner Approval’

The Impact of IDM!

Key Takeaways
- $582,492 realized annually in cost savings or cost avoidance
- More than 13,000 staff hours recovered annually
- Significant improvements in user customer service & customer satisfaction
Protect.

‘Lock Down and Protect’ Applications

- Secure, Risk-Based Single Sign On
- Automate User & Responsibility
- Automate Self Service Password Reset and Account Requests
- Preventative Segregation of Duties Controls
- Strong Access Controls and Data Protection
- Web-Based Periodic Access Review

Automate

Protect

Leverage Extend Automate Protect
**Strong Access Controls and Data Protection**

We need fine-grained access control of application data (at the UI and database levels).

We can’t ensure the protection of our applications' database data and prove controls are working.

**Solution**

- [Web Tier Oracle Access Suite](#)
- [Application (Internal) Identity Manager and GRC Controls](#)
- [Oracle Database Database Security IdM Suite](#)
- [Unix Host OS Oracle Application Services for OS](#)

---

**Protecting Oracle Applications**

*Top to Bottom Security*

- Protect the “Front Door” and provide strong fraud prevention using Oracle’s Access Management Suite
- Embed Fine-Grained Access controls down to the field level using Oracle Application Access Controls Governor
- Centralize OS User management and SUDO Policies using Oracle Authentication Services for Operating Systems

- Automatically add, modify and remove user accounts and entitlements using Oracle Identity Manager
- Secure sensitive data within the database with Oracle Database Security Options

---
‘Lock Down and Protect’ Applications

Preventative + Detective Segregation of Duties

Issue to Address:
- Segregation of Duties (SoD) within Applications is difficult to achieve even at a ‘detective’ level
- We want both Preventative & Detective SoD of Application entitlements

Solution:
- Oracle Identity Manager
- Oracle Application Access Controls Governor

Leverage, Extend, Automate, Protect
IDM and GRC Working Together

‘Proactive’ SoD Compliance means Simplified Compliance!

[Diagram showing the integration of IDM and GRC systems]

‘Lock Down and Protect’ Applications

[Diagram showing various applications and security controls]

ORACLE APPLICATIONS

Leverage Extend Automate Protect
Web-Based Periodic Access Review

Issue to Address:
- “Who has” & “Who had access to what?” and “Why?” reports are manual and time-consuming.
- We can’t detect and eliminate orphaned/ghost accounts. There could be thousands.
- Out of all these issues, periodic access reviews are the most complex, costly & time-consuming.

Solution:
- Oracle Identity Manager
- Option: GRC Suite

Periodic Reviews and Compliance Reporting

Complete System Right Out-of-the-Box

Oracle Identity Manager:
- “Web-Based & Actionable” Periodic Access Review
- Reports - Current & Historic “Who Has Access to What?”
- Reports - “Who Approved Each Access Request?”
- Rogue Account Detection, Reporting & Removal
- Oracle BI Publisher for Compliance Reporting

Employees & Contractors
Managers
Resource Owners
Security & Auditors

Oracle Database

Applications
Directories
Databases
Web-Based “Actionable” Access Reviews

22 Out-of-the-Box “Current State” Reports
13 Out-of-the-Box “Historical” Reports

### Historical Reports

The following is a list of historical reports that you can run:

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Report Code</th>
<th>Report Type</th>
<th>Report Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Membership History</td>
<td>UserMembershipHistory</td>
<td>Historical</td>
<td>Temporal history of user's memberships in user groups</td>
</tr>
<tr>
<td>User Resource Access History</td>
<td>UserAccountHistory</td>
<td>Historical</td>
<td>Temporal history of user's resource access</td>
</tr>
<tr>
<td>Task Assignment History</td>
<td>TaskAssignmentHistory</td>
<td>Historical</td>
<td>Temporal history of task assignments</td>
</tr>
<tr>
<td>Account Activity in Resource</td>
<td>AccountActivity</td>
<td>Historical</td>
<td>Account activity in resource</td>
</tr>
<tr>
<td>Users Created</td>
<td>UserCreated</td>
<td>Historical</td>
<td>Users Created in Specified Time Interval</td>
</tr>
<tr>
<td>Users Locked</td>
<td>UserLocked</td>
<td>Historical</td>
<td>Users Locked in Specified Time Interval</td>
</tr>
<tr>
<td>User Profile History</td>
<td>UserProfileHistory</td>
<td>Historical</td>
<td>Temporal history of user profiles</td>
</tr>
<tr>
<td>Users Disabled</td>
<td>UserDisabled</td>
<td>Historical</td>
<td>Users Disabled in Specified Time Interval</td>
</tr>
<tr>
<td>Users Created</td>
<td>UserCreated</td>
<td>Historical</td>
<td>Users Created in Specified Time Interval</td>
</tr>
</tbody>
</table>

Unified Compliance Reporting

**Using Oracle BI Publisher**

1. **Pull Data from Source**
2. **Business User Creates/Edits Layout Using Common Office and Adobe Tools**
3. **Output to Desired Formats**
4. **Send to Destinations**

- E-mail
- Printer
- Fax
- Storage
Leverage.

Provision & Access Accounts ‘Enterprise-Wide’

- Provisioning Manager
- Oracle Identity Manager
- Oracle Access Manager
- Applications
- Databases & OS/Legacy
- E-Mail
- Portals
- Physical Items

HR & Biz Applications
Other Sources
Flat Files
Databases
Directories

Suppliers
Employees
Customers
Customers Success with Oracle IDM
Benefits They Are Receiving

- PeopleSoft HR as source of truth for identity
- Eliminated > 90% of ghost, orphaned and rogue accounts
- Self-service password management reduced help desk calls
- Over $750,000 annual savings in help desk cost
- Saving $500,000 (400 hours/month) on SAP administration
- High quality IT compliance data for core SOX applications
- Over 1,100 applications under centralized management
- Comprehensive “Who has (and had) access to what” database for compliance and process automation
- “Near Zero” wait for new resources
- Embedded Application “Preventive, Detective and Contextual” Controls manage over 358 Business Processes
- 42% reduction in external auditor testing
- Less than 5 months payback period

Summary
Oracle is #1 in IDM with “Big 3” Analysts!!

FORRESTER

The Forrester Wave™: Identity And Access Management, Q1 2008

Automate Extend

Protect

Leverage

Gartner

Oracle is #1 in IDM with “Big 3” Analysts!!

User Provisioning Magic Quadrant

Web Access Management Magic Quadrant

This Magic Quadrant graphic was published by Gartner, Inc. as part of a larger research note and should be evaluated in the context of the entire research report. The Gartner report is available upon request from Oracle.
Oracle is #1 in IDM with “Big 3” Analysts!!

Oracle IDM is the “Best and Safest Choice” for Oracle customers

Only Oracle Provides...

Most Comprehensive:
- End-to-End Security for Applications, Middleware and Databases!
- Industry’s #1 IdM according to Gartner, Burton and Forrester reports

Deepest Set of Capabilities:
- HR-Driven, Role-based Oracle Application user management
- Deepest Integration for Management of Users, Roles and Entitlements
- Out-of-the-Box Single Sign-On to Oracle Applications
- Self-service Home Page for requesting/removing access requests
- Out-of-the-Box, Approval workflows per user access requests

Unmatched Compliance Options:
- “Actionable”, Periodic Review of Users and fine-grained entitlements
- Proactive and Detective SoD with remediation (IdM and GRC)
- Fine-Grained Access control down to the form/field level
- Database Vault to secure sensitive application data in the database
- Current and Historical Reporting of “Who has what responsibility?”, “When did they get it?”, “How did they get it?” and “Who approved it?”
"Leap Forward" with Oracle Identity Management for Oracle Applications

- **Leverage** - Your Oracle Application investment
- **Extend** - Its capabilities to solve common security problems, drive down costs and boost end user productivity
- **Automate** - Costly and Time-Consuming User Management, User Access, Access Recertification and Reporting processes
- **Protect** - Your Oracle Application “to the Core” with strong access controls, segregation of duties and data protection

Oracle Identity Management Activities

**Collaborate 09** - May 3 through May 7 in Orlando, FL
  - Website: [http://collaborate09.com/](http://collaborate09.com/)

**Sessions:**
  - May 6th, 11am-12pm - "Using Oracle Adaptive Access Manager to Detect and Prevent Fraud in Oracle Applications"
  - May 6th, 4:30pm-5:30pm - "Using Governance, Risk and Compliance Solutions to Achieve Segregation of Duties with Oracle Identity Management"

**Product Demonstrations**
  - Exhibit Hall, May 4 - 6

**Hands On Lab**
  - May 5th, 3:15pm - 5:15pm
  - "Automate, Secure, and Audit Your E-Business Suite and PeopleSoft Applications with Oracle Identity Management"
  - [Click Here to Register Now](http://collaborate09.com/)

**More Information: Viewlets and Whitepapers**
  - Oracle Fusion Middleware Best Practice Centers
“Leap Forward” with Oracle Identity Management for

Mini-Cast #1
Simplify User and Password Management

Mini-Cast #2
Simplify and Strengthen User Access

Mini-Cast #3
Simplify Governance, Risk and Compliance

Questions?

Chris Fox, CISSP
Principal Security Consultant
Oracle Identity and Security Team
chris.fox@oracle.com
ORACLE IS THE INFORMATION COMPANY