

Oracle Identity & Access Management

USTRANSCOM
September 28, 2016

ORACLE®

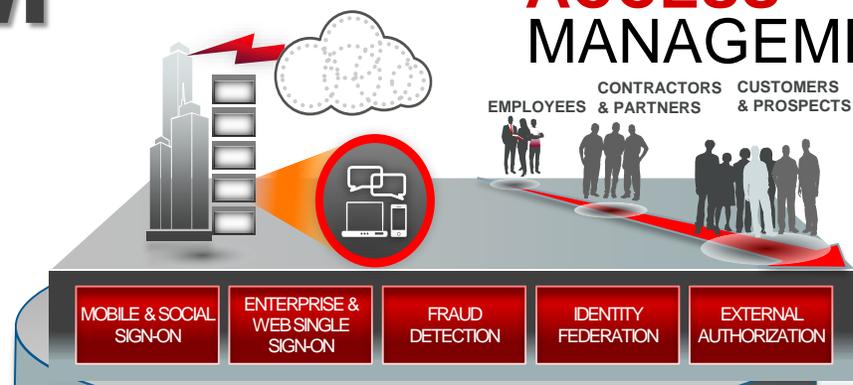
Copyright © 2014 Oracle and/or its affiliates. All rights reserved. |

Safe Harbor Statement

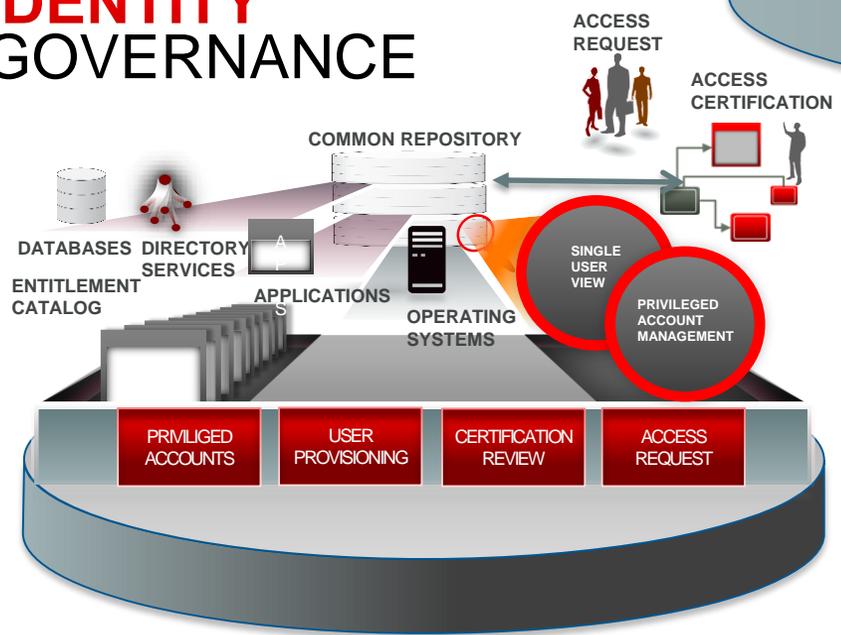
The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

INTEGRATED PLATFORM

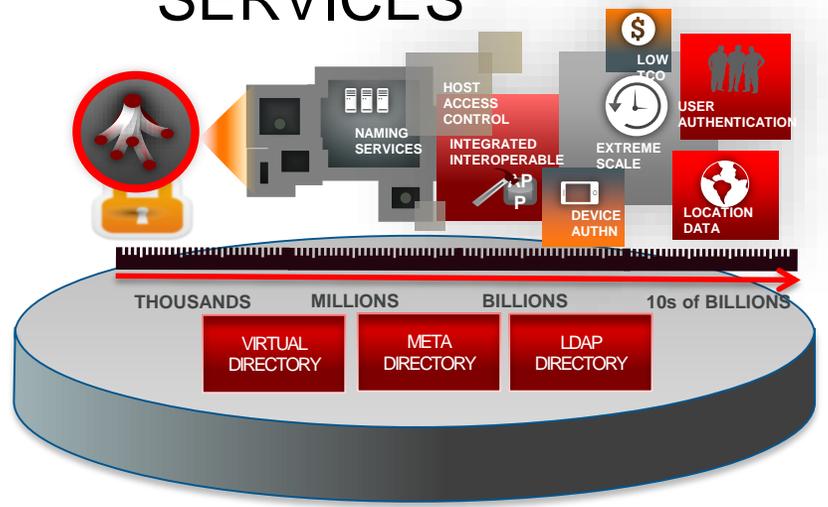
ACCESS MANAGEMENT



IDENTITY GOVERNANCE



DIRECTORY SERVICES



Oracle Access Management

Oracle Fusion Middleware's Security Pillar



Web



Mobile



Social



Internet of Things

Authentication

Intelligent, Risk-based
Strong Authentication

Authorization

Real-Time, Context-Aware
Externalized Policies

Federation

Standards-Based
Leverages Social Identities

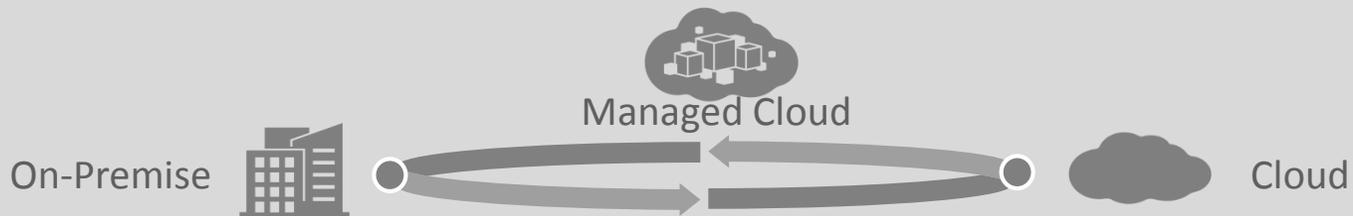
Mobile and API

RESTful Interfaces
API Security

Common Policy Model – Shared Infrastructure Services

Scalability, High Availability, Disaster Recovery

System Management



Oracle Access Management

Services and Capabilities



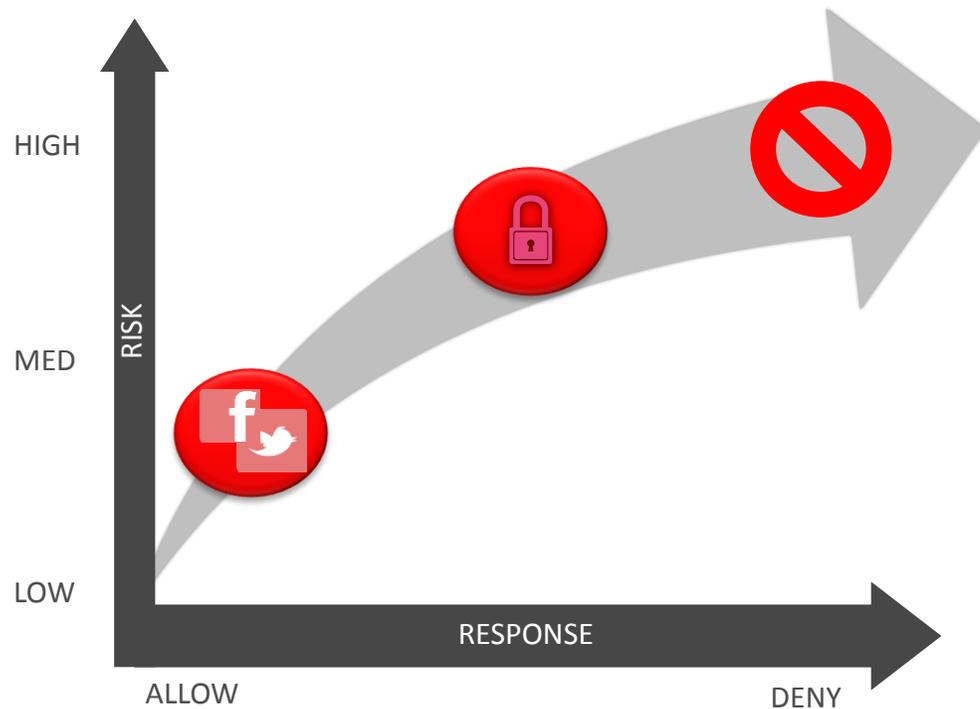
- Complete
- Context-aware and risk-aware
- Scalable, highly available
- Standards-based and modular

Access Management – Web SSO



- Web authentication
 - User name and password
 - Windows native authentication (WNA)
 - Strong authentication (CAC / PIV)
 - Multi-Factor
- Web Single Sign-On (SSO)
- Fine-grained authorization

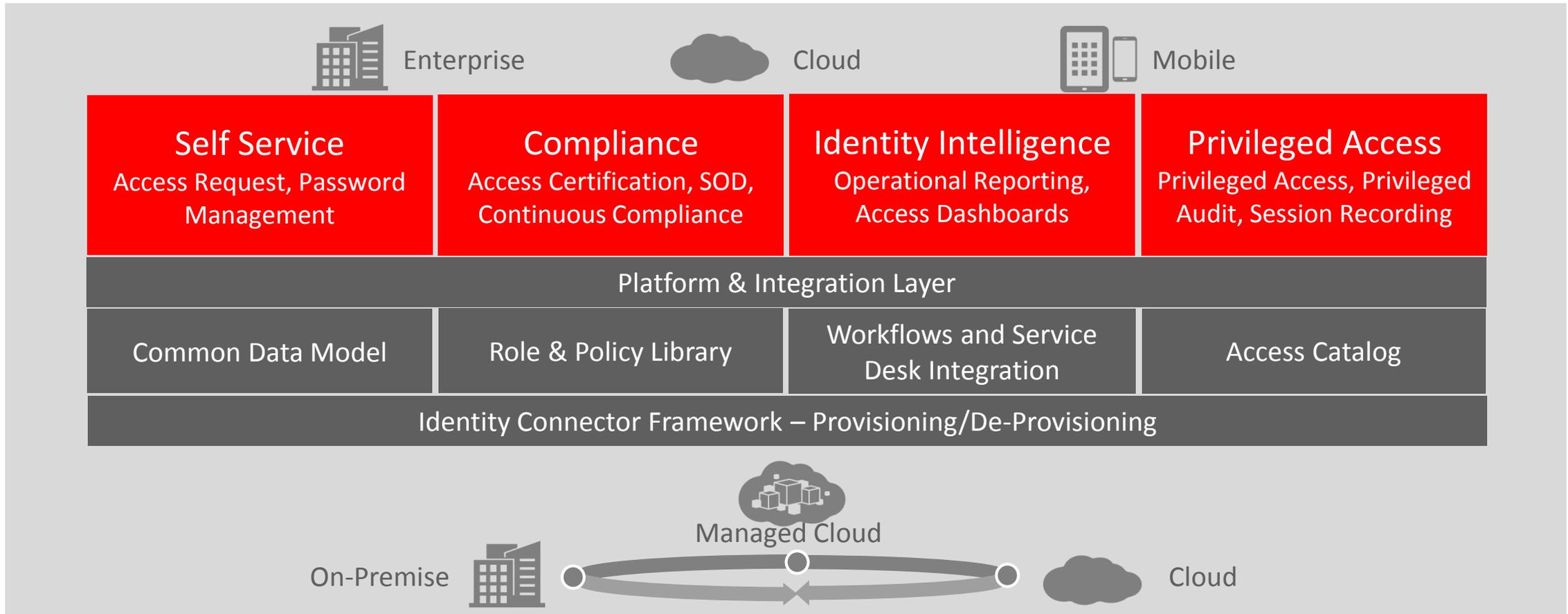
Integrated Risk, Fraud, and Strong Authentication



- Context-aware, risk-aware and content-aware
- Leverage real-time context for authentication and authorization
- Native mobile OTP for step-up authentication
- Real-time risk analysis and fraud prevention
- Data redaction through dynamic authorization based on risk
- Cross-platform consistent policies; adaptive to context, content and risk

Oracle Identity Governance

Unified Approach to Complete Identity Governance



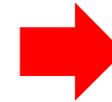
Business-Friendly Request Catalog

Enabling end-users to get the access they need

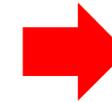
- Business-friendly Access Catalog
- Self-Service Application On-boarding And Administration
- Search, Browse And Contextual Recommendations
- In-line Policy Checks To Prevent SOD Violations
- Flexible Forms For Advanced Data Capture
- End-to-end Visibility Into The Approval and Fulfillment Process



**Business-Friendly
Access Catalog**



**Search,
Browse,
Recommend**



**Policy-compliant
Access Request**

Oracle Identity Governance

Intelligent Access Catalog

The screenshot shows the Oracle Identity Self Service interface for an Access Request. The page includes a search bar, filters for Type (All, Application, Role), Category, and Risk Level. A list of search results is displayed with 'Add to Cart' buttons. The user is identified as Lee Baker.

Refine Results	Item	Info	Action
Categories	Base account in Financials 12.1	i	+ Add to Cart
Applications (3)	Vision Payables Manager	i	+ Add to Cart
Entitlements (3)	Vision HR - Benefits Analyst	i	+ Add to Cart
Role (4)	Sharepoint Employee Access	i	+ Add to Cart
My Category (4)	Site Scope Reporting Publisher	i	+ Add to Cart
	Employee Benefits Portal Content Editor	i	+ Add to Cart
	Employee Benefits Portal Content Manager	i	+ Add to Cart
	Employee Benefits Portal Viewer	i	+ Add to Cart
	Base account in Financials 12.1	i	+ Add to Cart

1 to 6 of 20 | Next Page

- Access Catalog provides ability to browse and search
- Smart search forms allow users to navigate the Catalog in a guided manner
- Catalog search results indicate relevance
- Access Catalog can recommend access based on pre-defined and user-defined criteria
- Support for Start/End Dates for Access Grants
- Preventative SoD Analysis

Oracle Identity Governance

Comprehensive Role Lifecycle Management

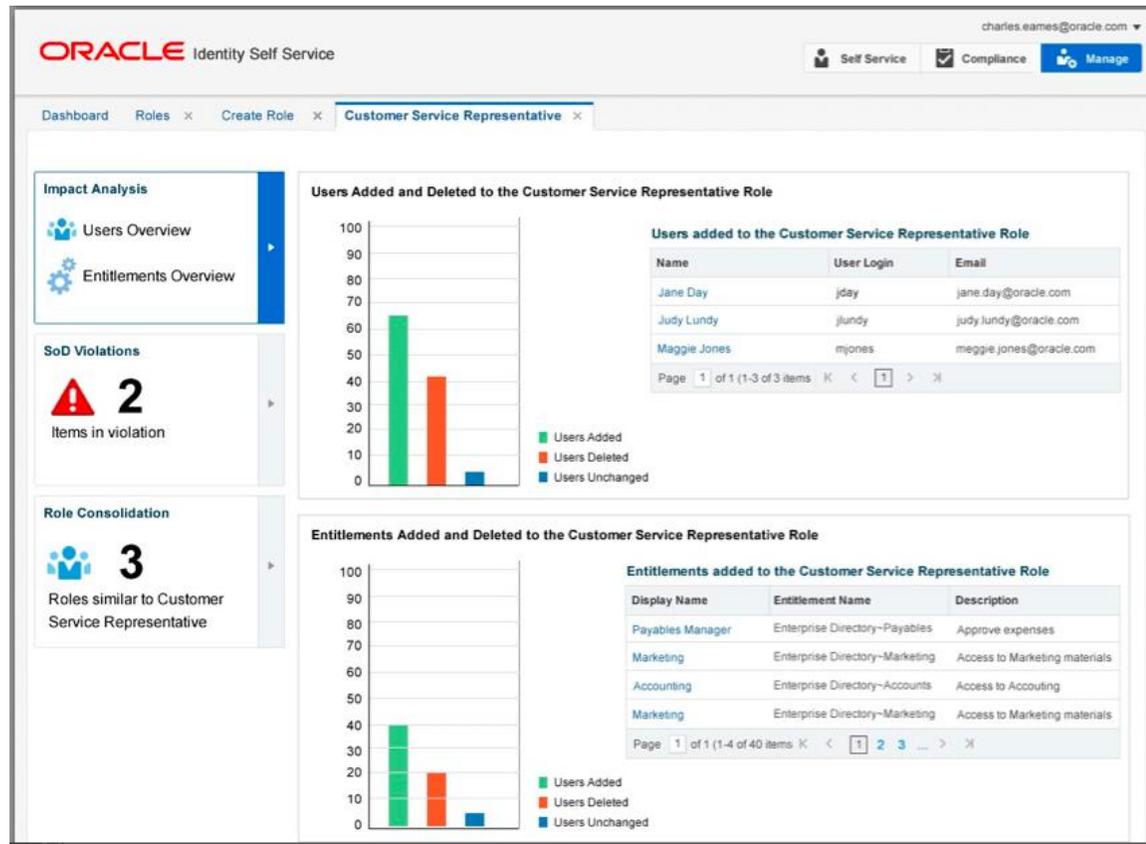
The screenshot shows the Oracle Identity Self Service interface for creating a new role. The user is logged in as charles.eames@oracle.com. The navigation bar includes 'Self Service', 'Compliance', and 'Manage'. The 'Create Role' process is shown as a multi-step wizard with steps: Attributes, Hierarchy, Access Policy, Members, Organizations, and Summary. The 'Attributes' step is currently active. The form fields are as follows:

General Role Information	
* Name	Customer Service Representative
Display Name	Customer Service Representative
Email	csrep@oracle.com
Description	Customer Service Rep with Access to EBS Application
Role Category	Privileged Role
Owned By	Hatori Hanzo
Audit Objective	SOX Critical
Risk Level	Low
User Defined Tags	Role, CSR, Rep II
Approver User	Hatori Hanzo
Approver Role	None
Certifier User	Hatori Hanzo
Certifier Role	None
Fulfillment User	Danny Crane
Fulfillment Role	None
Certifiable	<input checked="" type="checkbox"/>

- Business users can request creation of new roles and changes to existing ones
- Role requests can leverage the same request and approval framework available for Access Requests and Certification
- Role owners can see comprehensive auditing and prior versions

Oracle Identity Governance

Comprehensive Role Lifecycle Management



- Comprehensive role analytics allows business users to see the impact of new roles and changes to existing ones
- Role owners can reduce role explosion by review the effectiveness of the roles and consolidate new roles with existing ones
- Business users can create roles using “model users”

Oracle Identity Governance

SOD Detection and Closed Loop Remediation

The screenshot displays the Oracle Identity Governance SOD Analysis interface. The main window is titled "EBS Dev SOD Analysis" and is divided into two tabs: "Details" and "Action History".

Violation Details:

Policy	EBS Dev SOD Analysis	User Name	ethorne
Description	Short description goes here.	Full Name	Emma Thorne
Assigned To	Conway, Brad	Employee ID	12345
Assigned Date	January 22, 2014	Email	emma.thorne@oracle.com
State	Open	Title	HR Specialist II
Detection Count	1	Organization	Human Resources
Last Detected	01/22/2014	Manager	Conway, Brad
Expiration Date	02/14/2014		
Comments	User: violation created by saving preview		

Access Details:

Rules Violated:

- US Employees
- EBS Administrator
- Administrators Payroll
- Works for Acme
- Has EBS Dev Account

Violation Cause Table:

Violation Cause	Status	Attributes	Comments
roleName = Account Manager	Active	Role Name Account Manager	
applinstance = DEV103	Active	Resource EBS Application Instance DEV103 Account Name emmaEBS01	
organizationName = Human Resources	Active		
applinstance ['DEV103'].entitlement = ebsAdmin7	Active		

- SOD Rule and Policy Definition
 - Define rules across users, applications, roles and entitlements
- Detective SOD Analysis
 - Detective Policy Enforcement – Closed Loop Remediation
 - Access History to audit all violations and decisions
 - Review High Risk policy violations in Certifications
- Preventative SOD Analysis
 - Enforce SOD policies during access requests
 - Review policy violations during approvals and launch exception workflows

Oracle Identity Governance

Simplified yet granular security

The screenshot displays the Oracle Identity Self Service interface for creating an admin role. The breadcrumb trail is Home > Manage > Authorizations > Create Admin Role. The main content area is titled 'Create Admin Role' and features a progress bar with steps: Attributes, Capabilities, Members, Scope of Control, Organizations, and Summary. The 'Capabilities' step is active, showing a search bar and a shuttle interface between 'Available Roles' and 'Selected Roles'. The 'Available Roles' list includes 'Create User', 'Modify User', 'Lock User', and 'Unlock User'. The 'Selected Roles' list includes 'Create User', 'Modify User', 'Lock User', and 'Unlock User'. A 'Create User' dialog box is open, showing a 'Select Attributes' list with checkboxes for 'First Name', 'Last Name', 'Department', 'Location', 'Email Address', 'Password', and 'Organization'. The dialog box has 'Add' and 'Cancel' buttons.

- Administrators can define custom security roles to control who can do what at an attribute level
- Users can be assigned security roles via rules reducing administration burden
- User actions and the context that they used to perform the action are audited

Oracle Privileged Account Manager

Accountability

- Check-Out / Check-In Self Service Console
- Custom built approvals (e.g. phone)
- Custom built ticketing system integration
- Custom built notifications
- Access Request Interface – Privilege Accounts added to OIG resource catalog
- Keystroke logging
- Session recording

OPAM

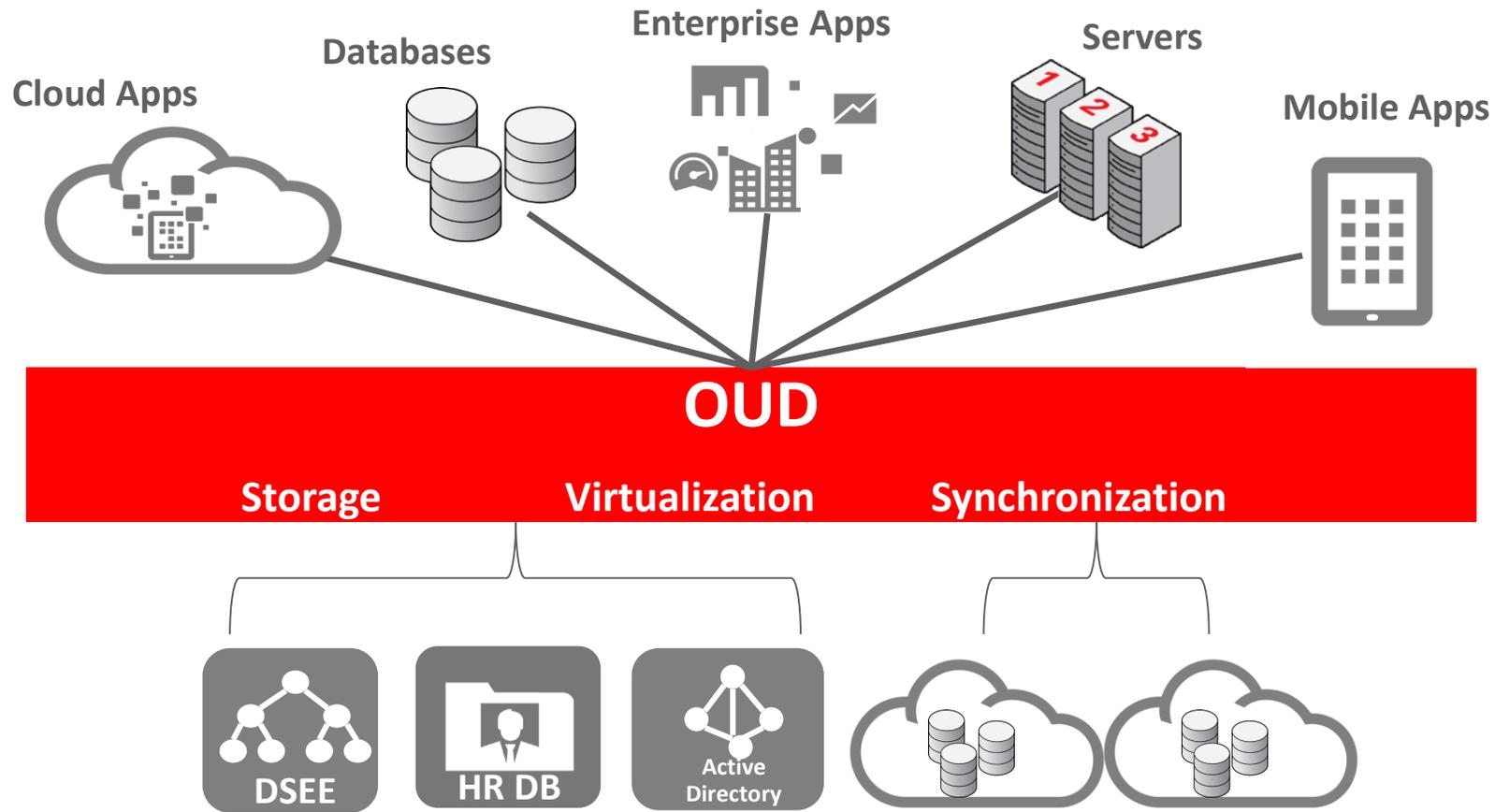
More managed targets, greater control and more visibility

The screenshot displays the Oracle Privileged Account Manager (OPAM) web interface. The top navigation bar includes 'ORACLE Privileged Account Manager', 'Accessibility', 'Help', 'Sign Out', and 'opam_admin'. The left sidebar contains navigation menus for 'Home', 'Administration', 'Reports', and 'Configuration'. The main content area is divided into two panes. The top pane, titled 'Checkout History', features a search form with fields for 'Start Date', 'End Date', 'Account Name', 'User Name', 'Target Name', and 'Pattern', along with a 'Query Size' dropdown set to 25. Below the search form is a table with columns: Row, Start Date, End Date, Account Name, User Name, Target Name, and Recording. The table contains 9 rows of data. The bottom pane, titled 'Video Recording Player', shows details for a specific session: 'Account Name: SystemAdmin', 'Target Name: WindowsMachine', 'Start Date: Wed Jun 25 08:17:40 PDT 2014', 'End Date: Wed Jun 25 08:19:09 PDT 2014', and 'User Name: Olaf'. Below these details is a video player showing a desktop environment with various icons and a taskbar. A list of session events is displayed on the right side of the video player, including 'Program Manager', 'Start menu', 'Program Manager', 'New Tab - Google Chrome', 'The Official Website of the FIFA World Cup - FIFA', 'Start menu', 'Notepad', 'Start menu', 'Start', 'Snipping Tool', 'Notepad', 'The Official Website of the FIFA World Cup - FIFA.com', '2014 FIFA World Cup Brazil: Nigeria-Argentina - Overview', 'Start menu', and 'Program Manager'.

Row	Start Date	End Date	Account Name	User Name	Target Name	Recording
1	6/25/14 8:02 AM	6/25/14 8:08 AM	SystemAdmin	olaf	WindowsMachine	
2	6/25/14 8:04 AM	6/25/14 8:05 AM	SystemAdmin	olaf	WindowsMachine	
3	6/24/14 8:10 PM	6/25/14 8:01 AM	SystemAdmin	olaf	WindowsMachine	
4	6/24/14 9:45 PM	6/24/14 9:46 PM	SystemAdmin	olaf	WindowsMachine	
5	6/24/14 8:11 PM	6/24/14 8:16 PM	SystemAdmin	olaf	WindowsMachine	
6	6/24/14 2:28 PM	6/24/14 3:02 PM	SystemAdmin	olaf	WindowsMachine	
7	6/24/14 2:38 PM	6/24/14 2:38 PM	SystemAdmin	olaf	WindowsMachine	
8	6/24/14 9:37 AM	6/24/14 9:37 AM	SystemAdmin	olaf	WindowsMachine	
9	6/24/14 9:38 AM	6/24/14 9:38 AM	SystemAdmin	olaf	WindowsMachine	

- Extended managed targets
 - UNIX
 - LDAP
 - Database
 - Windows
 - SSH based targets
 - SAP
 - UNIX / Linux server
 - Oracle Database
 - Microsoft SQL Server
 - Sybase
 - IBM DB2
 - Microsoft Active DirectorySession Management control policies
- Session Recording

OUD – The All in One Directory



- Storage, virtualization and Sync
- High performance
- Extreme scalability
- REST support

Oracle Enterprise Manager Fusion Middleware Control

ORACLE Enterprise Manager 11g Fusion Middleware Control Setup Help Log Out

Farm

Logged in as weblogic Page Refreshed Mar 8, 2015 9:03:02 PM UTC

Farm_oam_domain

- Application Deployments
- WebLogic Domain
- Identity and Access
- Metadata Repositories
- Web Tier

Farm_oam_domain

Deployments

Name	Status	Target
Application Deployments		
Internal Applications		
oam_admin(11.1.2.0.0)	Up	AdminServer
oamsso_logout(11.1.2.0.0)	Up	AdminServer
oamsso_logout(11.1.2.0.0)	Up	oam_server1
omsm(11.1.2.3.0)	Down	AdminServer

Fusion Middleware

Name	Status	Host	CPU Usage (%)
WebLogic Domain			
oam_domain			
AdminServer	Up	oam.example.com	0.00
oam_policy_mgr1	Down		
oam_server1	Up	oam.example.com	0.00
Identity and Access			
OAM	Up		
oam_server(11.1.2.0.0)	Up	oam.example.com	
Metadata Repositories			
mds-owsm		oam.example.com	
Web Tier			
ohs7	Up	db.example.com	0.00
ohs8	Up	db.example.com	0.00
ohs9	Up	db.example.com	0.00

Farm Resource Center

Before You Begin

[Understanding Key Oracle Fusion Middleware Farm Concepts](#)

ORACLE®