INTEGRIGY

WebLogic
Security Top Ten

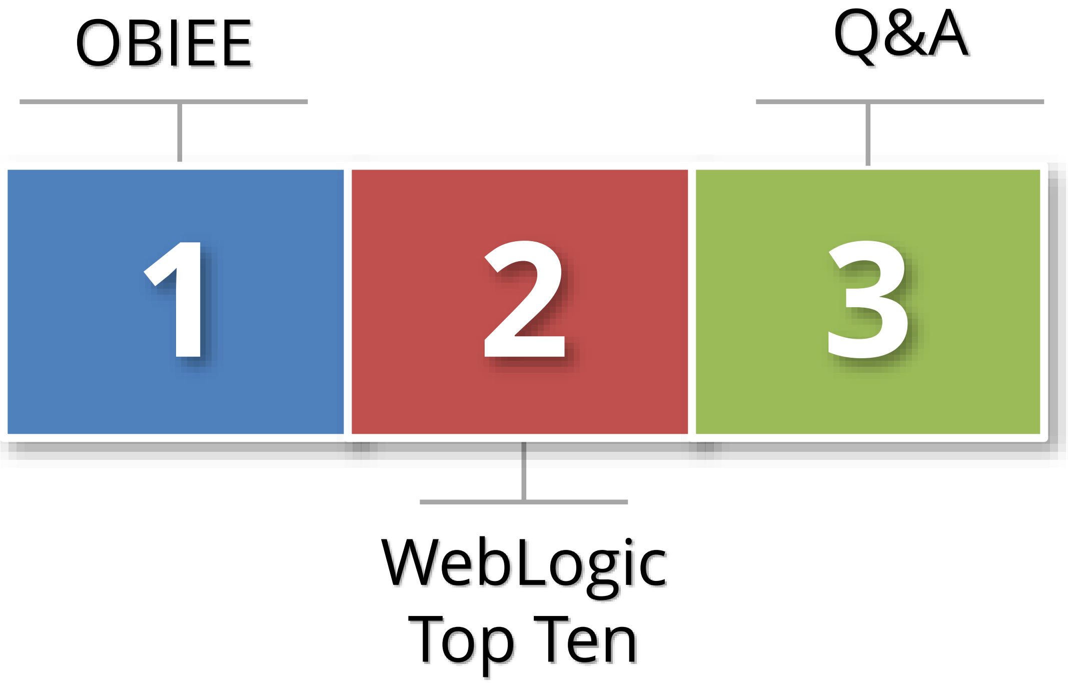
June 2014

Michael Miller
Chief Security Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Agenda

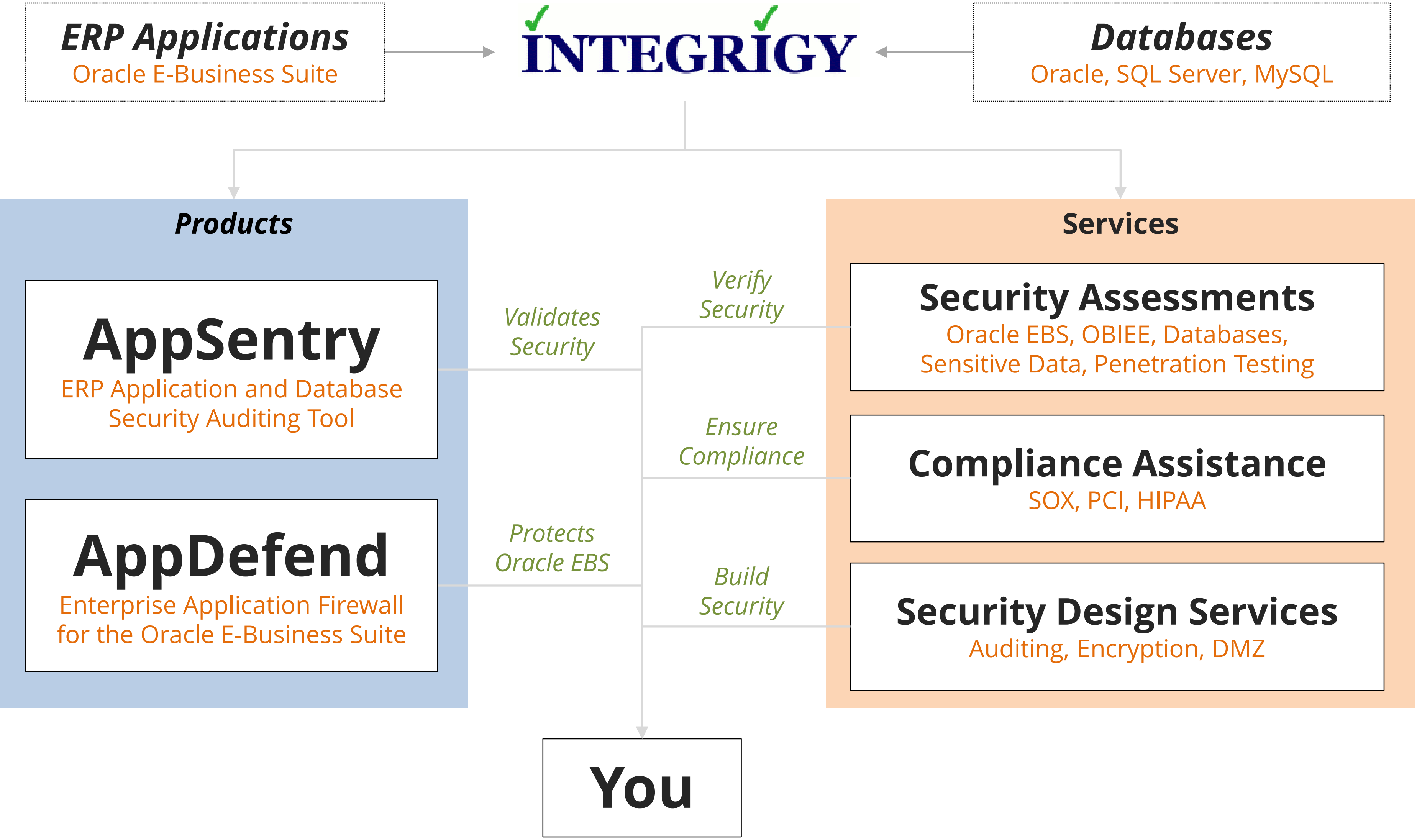


1 OBIEE

2 WebLogic Top Ten

3 Q&A

About Integrigy



ERP Applications
Oracle E-Business Suite

INTEGRIGY

Databases
Oracle, SQL Server, MySQL

Products

AppSentry
ERP Application and Database Security Auditing Tool

Validates Security

AppDefend
Enterprise Application Firewall for the Oracle E-Business Suite

Protects Oracle EBS

Services

Verify Security

Security Assessments
Oracle EBS, OBIEE, Databases, Sensitive Data, Penetration Testing

Ensure Compliance

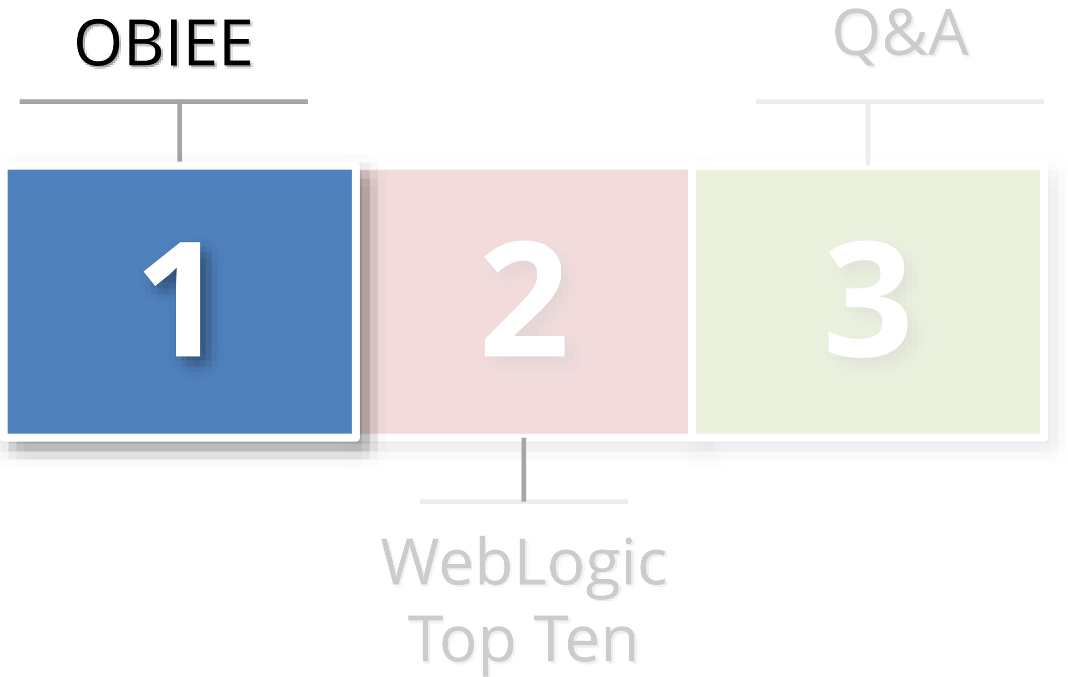
Compliance Assistance
SOX, PCI, HIPAA

Build Security

Security Design Services
Auditing, Encryption, DMZ

You

Agenda



OBIEE

1

2

WebLogic
Top Ten

3

Q&A

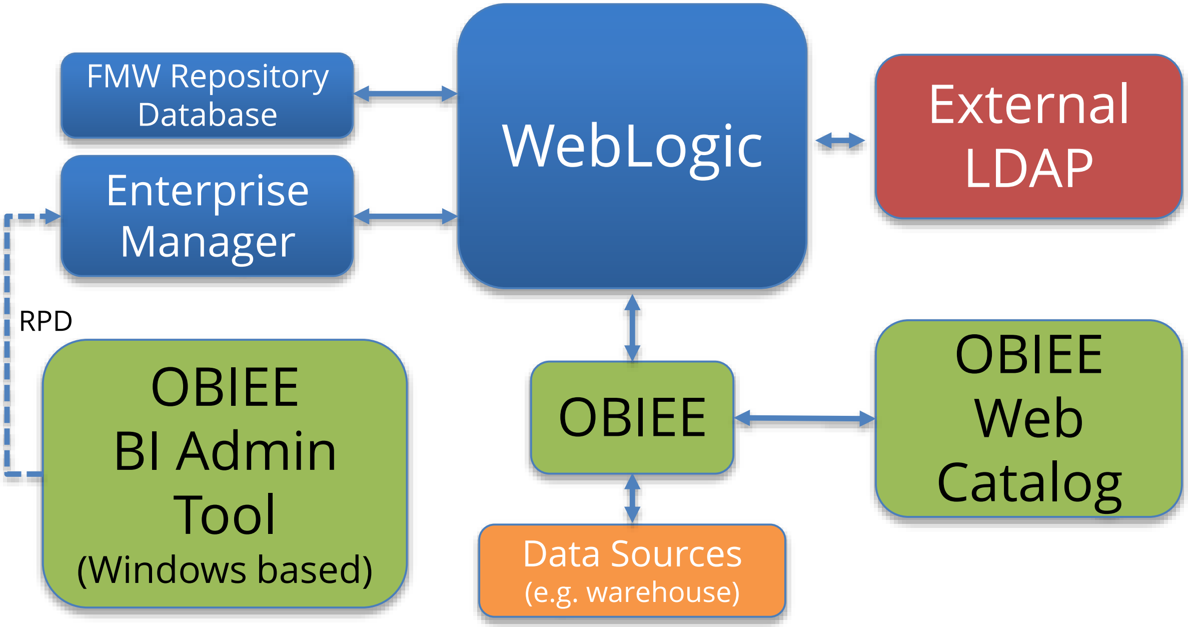
Facts About OBIEE Security

- **OBIEE is a Fusion Middleware product**
  - It is deployed within WebLogic

- **WebLogic security issues will make or break OBIEE security**
  - Far too often find the results of **Install-and-Run**

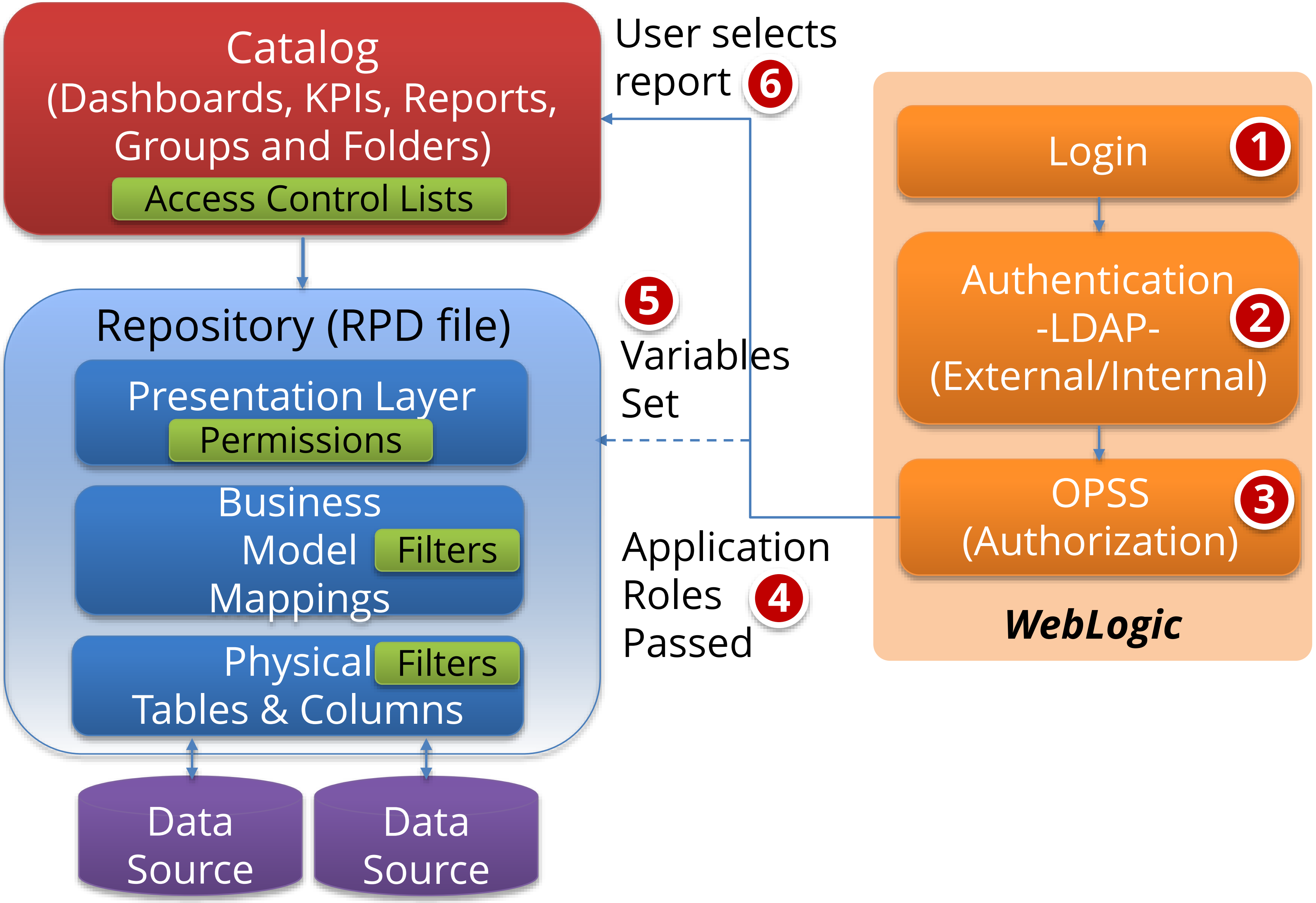
- **WebLogic is a complex product**
  - Database Administrators (DBA)s need to master new skills

OBIEE Security Examined



Size of box proportionate to component’s impact on security

OBIEE Security



Security Realms

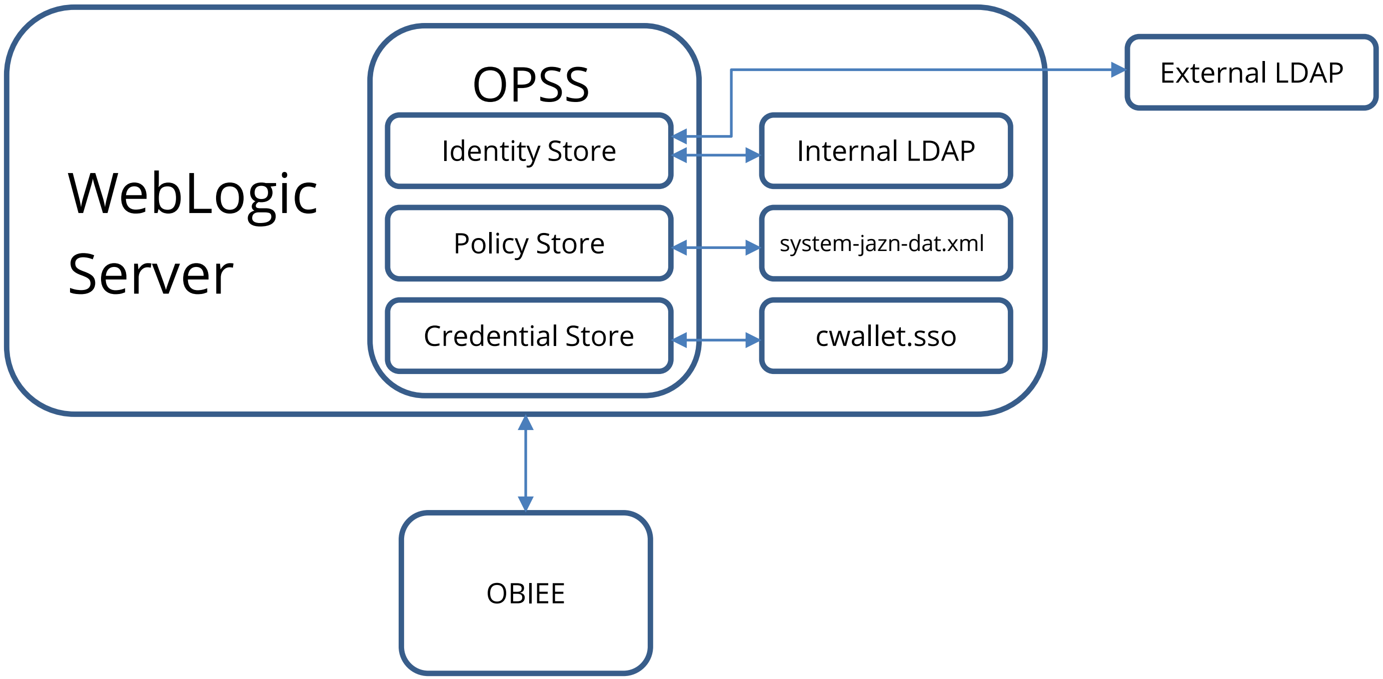
- **OBIEE 11g uses WebLogic for centralized common services**
  - Common security model included
  - Significant change from OBIEE 10g

- **WebLogic common security defined through security realms. Realms define:**
  - Users
  - Groups
  - Security roles and policies

- **Key decision**
  - Use default security realm or custom for OBIEE

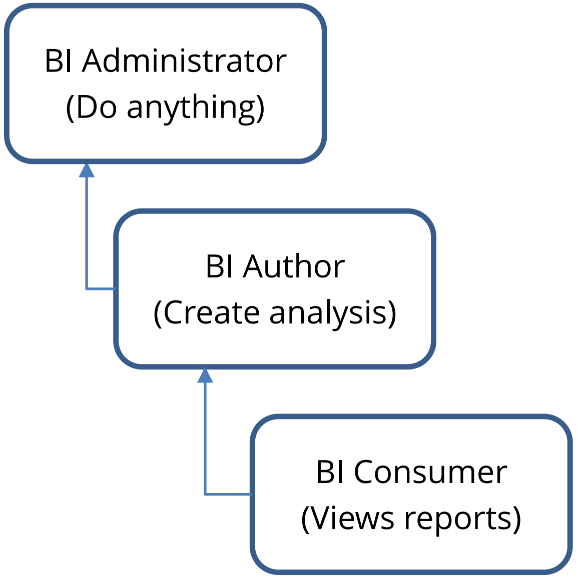
Oracle Platform Security Services (OPSS)

Transcends ALL Fusion Middleware Products

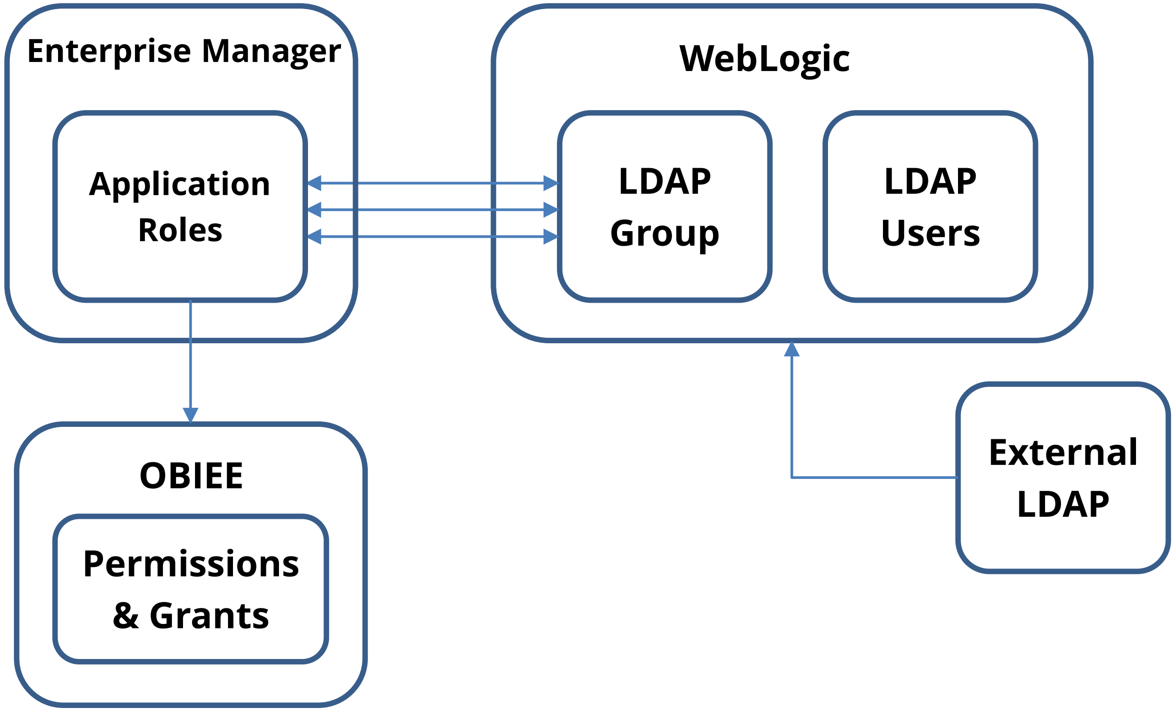


Application Roles

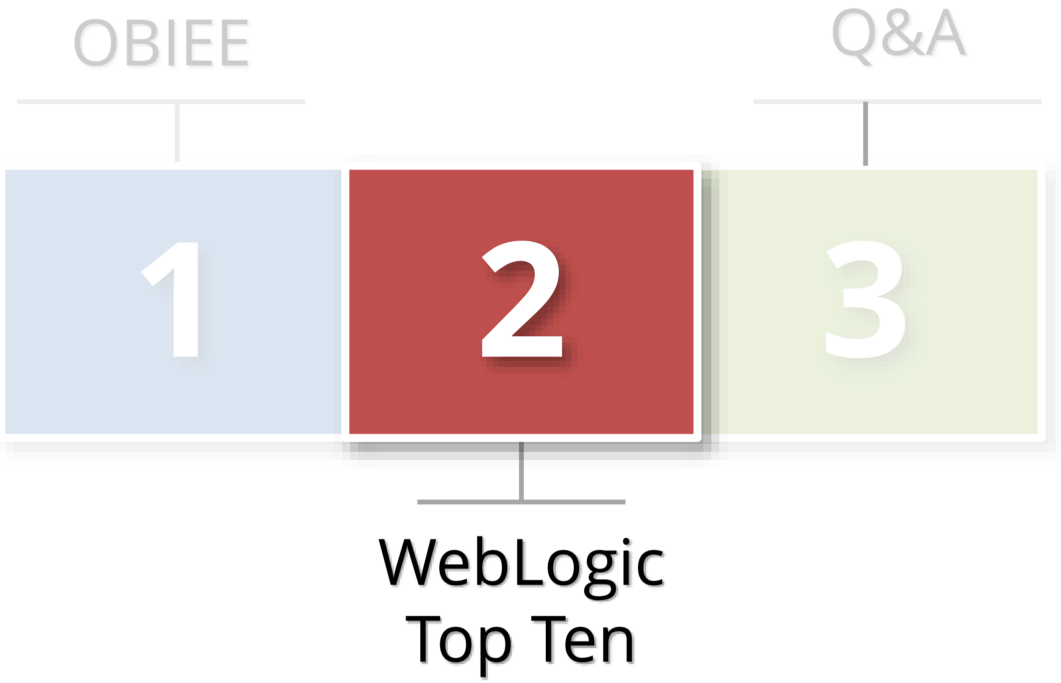
- **Transcend ALL Fusion Products**
- **Defined in Enterprise Manager**
- **Map to LDAP groups**
    - External or internal
- **Key Decision:**
    - Use default or custom



Applications Roles



Agenda



Top 10 WebLogic Security Vulnerabilities

- **List result of**
  - Client assessments
  - Integrigy's research

- **Selection criteria**
  - What can be pragmatically addressed or should be discussed
  - Risk of OBIEE information disclosure

Top 10 WebLogic Security Vulnerabilities

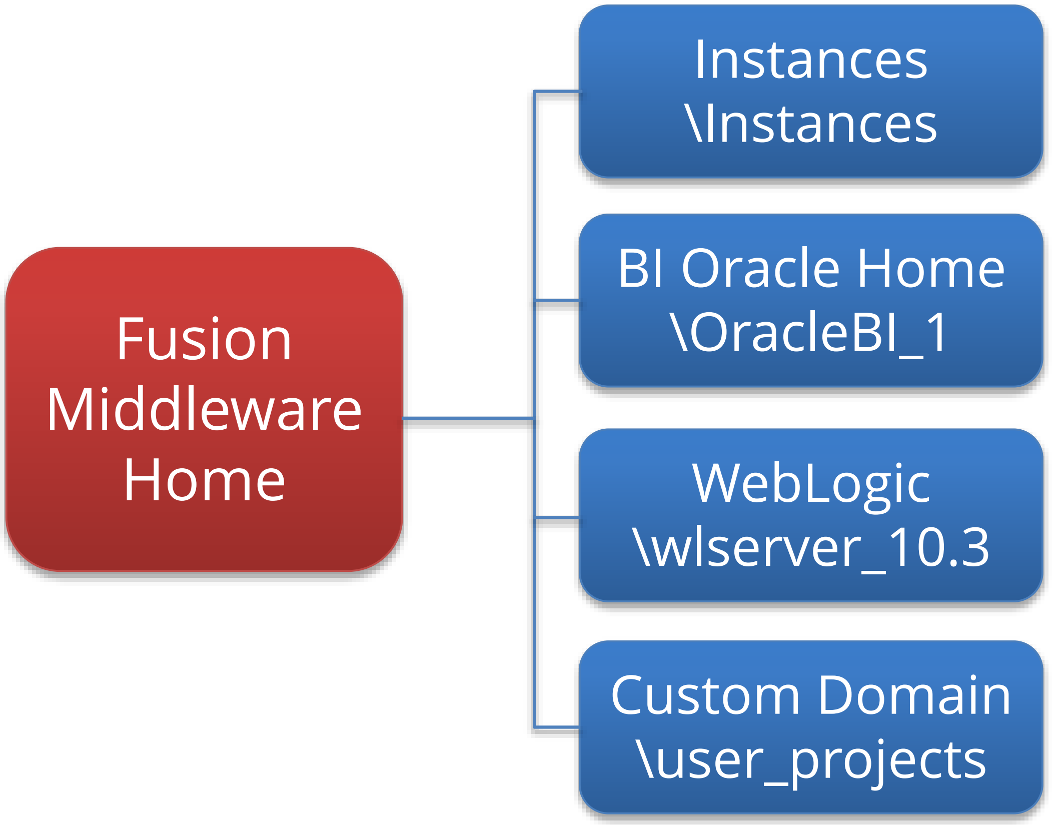
1. **Poor Patching Policies and Procedures**
2. **File system access**
3. **Running as privileged user**
4. **Not hardened**
5. **Too many WebLogic Administration users**
6. **Weak Change Control Procedures**
7. **No logging or auditing**
8. **Multiple authenticators**
9. **Metadata database not secure**
10. **WLST access and scripts**

Poor Patching Policies

- **10.3.5**
  - Released May 2011
  - Grace period ended August 2013
- **10.3.6**
  - February 2012
  - Grace period ends December 2021
  - Terminal patch set for 11g
- **CPU Patches**
  - WebLogic and Fusion Middleware
- **Java**
  - 1.6 vs. 1.7

WebLogic File System Access

- **Secure the underlying operating system**



RPD files, security ACLs, logs and config files

Binaries for OBIEE components

WebLogic binaries and WLST scripts

BI Domain Server configs, WLST scripts

WebLogic File System Access

- **Carefully limit people with file system access**
  - At a minimum, consider using umask 066 - other users may not modify or read files but may execute them where appropriate

- **Protect key configuration files**
  - For example (boot.properties, Weblogic.properties, fileRealm.properities)

- **Dated but still relevant WebLogic security guide from NSA (Unclassified)**
  - http://www.nsa.gov/ia/_files/webs/i33-004r-2005.pdf

Running WebLogic as Privileged User

- **Do not run WebLogic as root or privileged account**
  - Start WebLogic under the privileged user account, bind to the privileged ports, and then change its user ID to a non-privileged account
  - Start WebLogic using a non-privileged account and configure the firewall to use Network Address Translation (NAT) software to map protected ports to unprotected ones

Not hardened

- **Default WebLogic Security Realm used**
  - Create custom Realm or carefully understand default Realm and configurations

- **Production not clean**
  - Development and test done in production
  - Sample and demo applications installed in prod

- **Not using**
  - DMZ
  - Web Application Firewall or IDS/IPS
  - Virtual URL/Default URL

Not hardened

- **Web Robots page not configured**
  - Robots.txt

- **Powered By**
  - X-Powered-By not set to NONE

- **Test and development available**
  - Expose to Internet only as needed

Not hardened

- **Diagnostic and internal applications are externally accessible**
  - https://obieewebuat.yourcompany.com/dms
  - https://obieewebuat.yourcompany.com/wsm-pm
  - https://obieewebuat.yourcompany.com/AdminService
  - https://obieewebuat.yourcompany.com/bicontent

- **WebServices running externally**
  - https://obieewebuat.com:9704/analytics/saw.dll?WSDL

WebLogic Administration Users

- **Inappropriate WebLogic admin users**
  - Developers and staff outside of WebLogic admin team
  - Production access
  - Out-of-date
- **Local account governance**
  - Weak passwords
  - Rotation and expiry issues

Weak Change Control

- **Inconsistent OPSS practices**
  - Application roles and credentials
- **Migrations from non-production to production**
  - GUI or WLST?
- **Application deployment procedures**
  - OBIEE RPD (who, when and how?)

No WebLogic Logging or Auditing

WebLogic Auditing

- **Prebuilt compliance reporting features**
- **Common audit record format**
- **Flexible and extensive**
  - Specific criteria
  - Severity levels

Recommend

- **Log authentication history/failures**
- **Log authorization history**
- **Write audit data to:**
  - Database
  - File
- **Use audit data in**
  - BI Publisher
  - Splunk, ArcSight etc.…

Multiple Authenticators

- **Full identity defined in from one of multiple LDAP directories**
  - Provisioning/de-provisioning complexity
- **Partial identities supplied by more than one LDPA solution**
  - Provisioning/de-provisioning complexity

Metadata Repository Not Secured

- **Metadata repository database required for each Fusion Middleware product. OBIEE schemas:**
  - BIPLATFORM
  - MDS

- **Common Issues**
  - Access allowed
  - Passwords known, complexity, rotation
  - Not patched
  - No logging or auditing

WebLogic Scripting Tools (WLST)*

WLST

- **Command line scripting tool to manage WebLogic**
  - Jython based
- **On and offline modes**
  - Both are powerful
- **Access remotely or console**
- **WebLogic Security Framework enforces same rules as user interface**

Security Issues

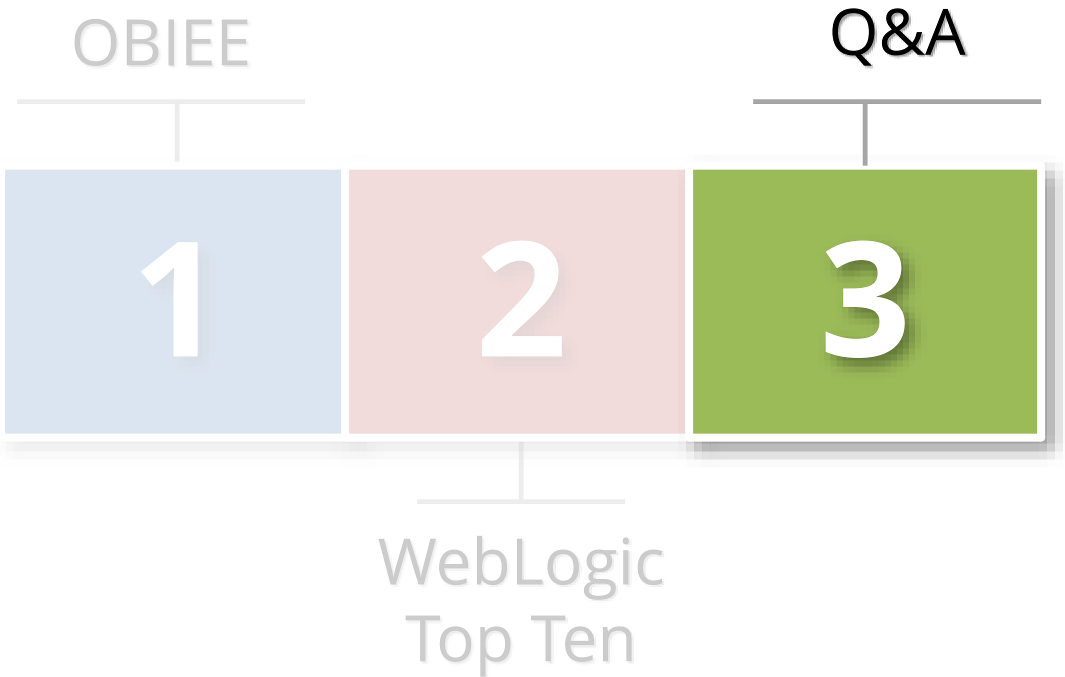
- **Not using administration port**
- **Inappropriate WebLogic accounts used in scripts**
- **Appropriate staff access to WLST scripts**
- **Hardcoded credentials**
- **Encrypted attributes exposed in scripts**
  - E.g. listCred()

* DBAs use SQL, WebLogic Admins use WLST

Java MBEANS Remote Access

- **Also called JMX/JConsole**
- **Remote access default is not secure**
  - **Anyone can update OBIEE**
  - **Anyone can update WebLogic**
- **Only need network access and port number**
  - No password required
- **Recommend**
  - Enabling password
  - Restricting remote access to read-only

Agenda



Contact Information

Mike Miller

Chief Security Officer

Integrigy Corporation

web: **www.integrigy.com**

e-mail: **info@integrigy.com**

blog: **integrigy.com/oracle-security-blog**