COLLABORATE14
TECHNOLOGY AND APPLICATIONS FORUM
FOR THE ORACLE COMMUNITY

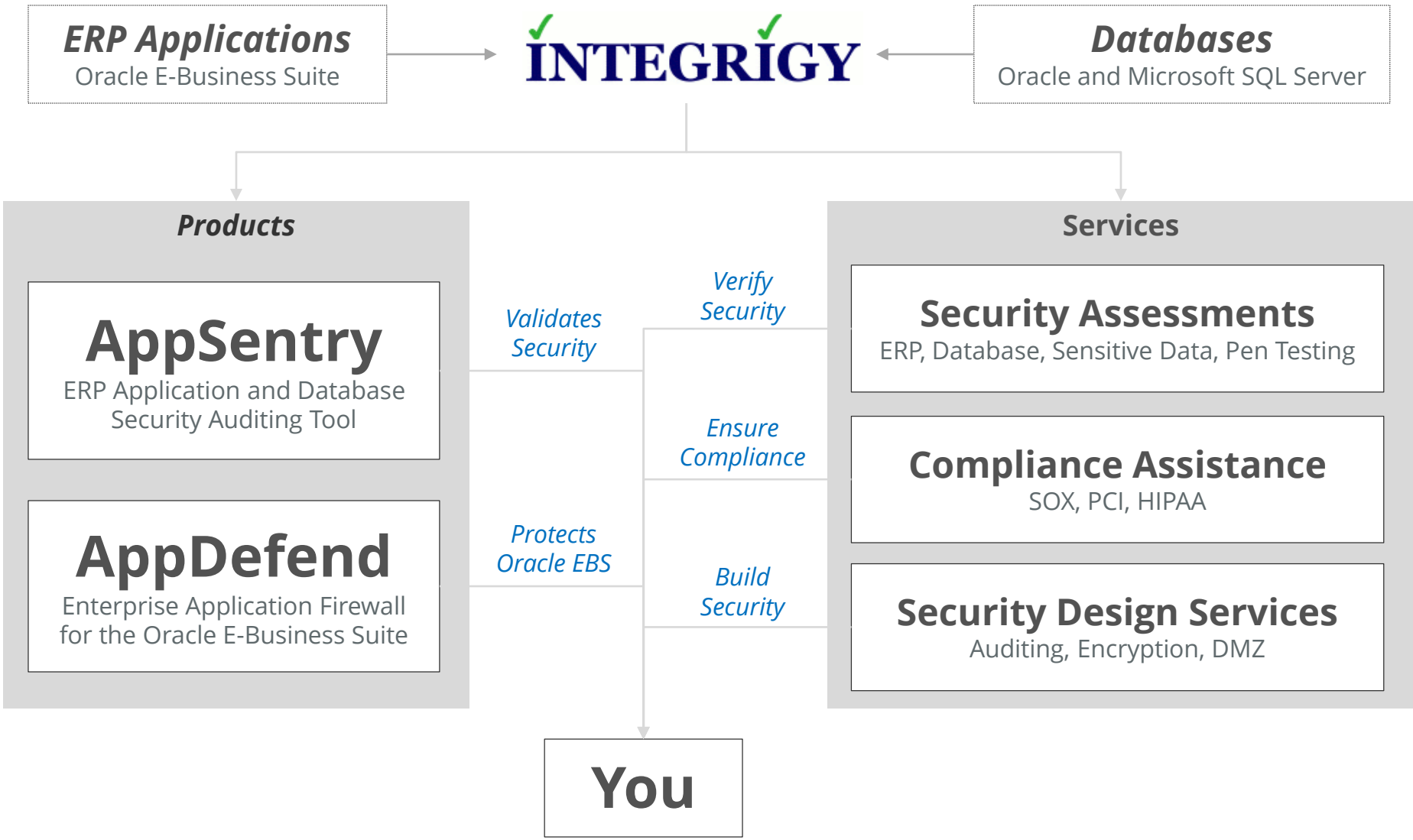
#C14LV

New Security Features in Oracle E-Business Suite 12.2

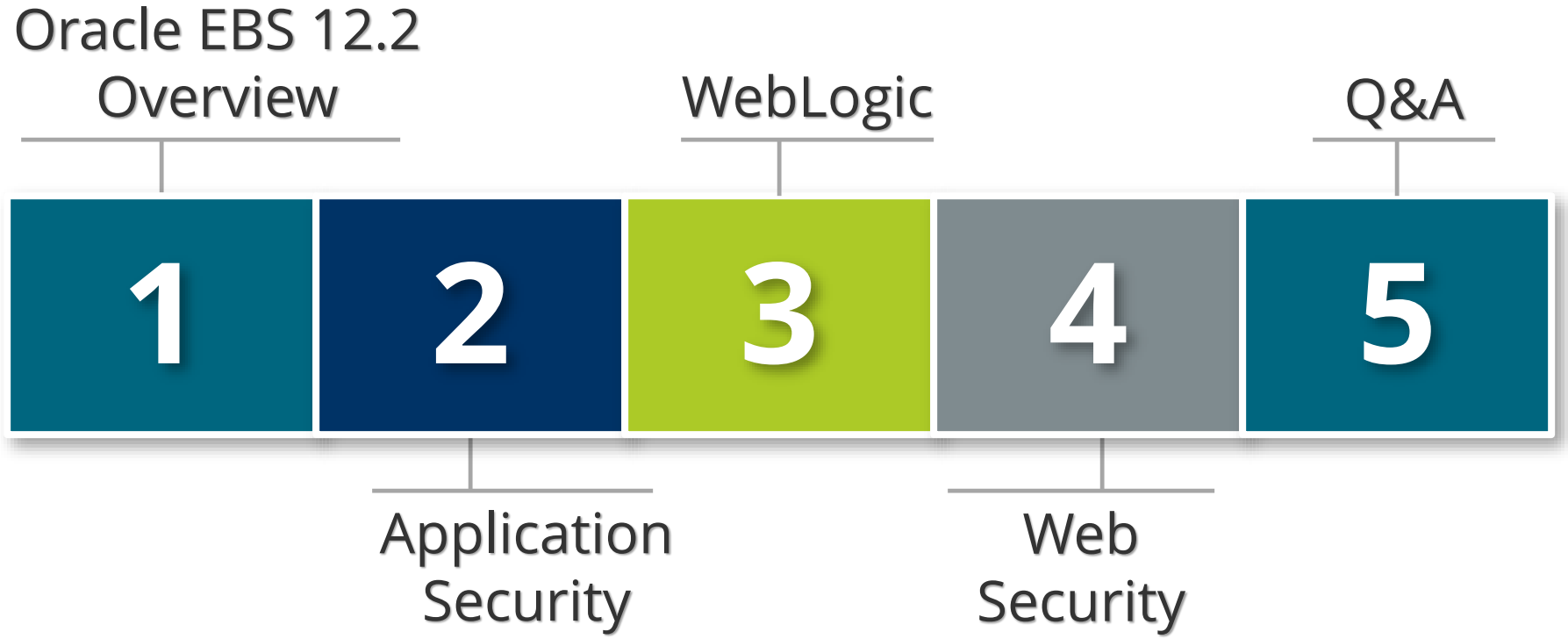
Session ID#: 14365

Stephen Kost
Chief Technology Officer
Integrigy Corporation

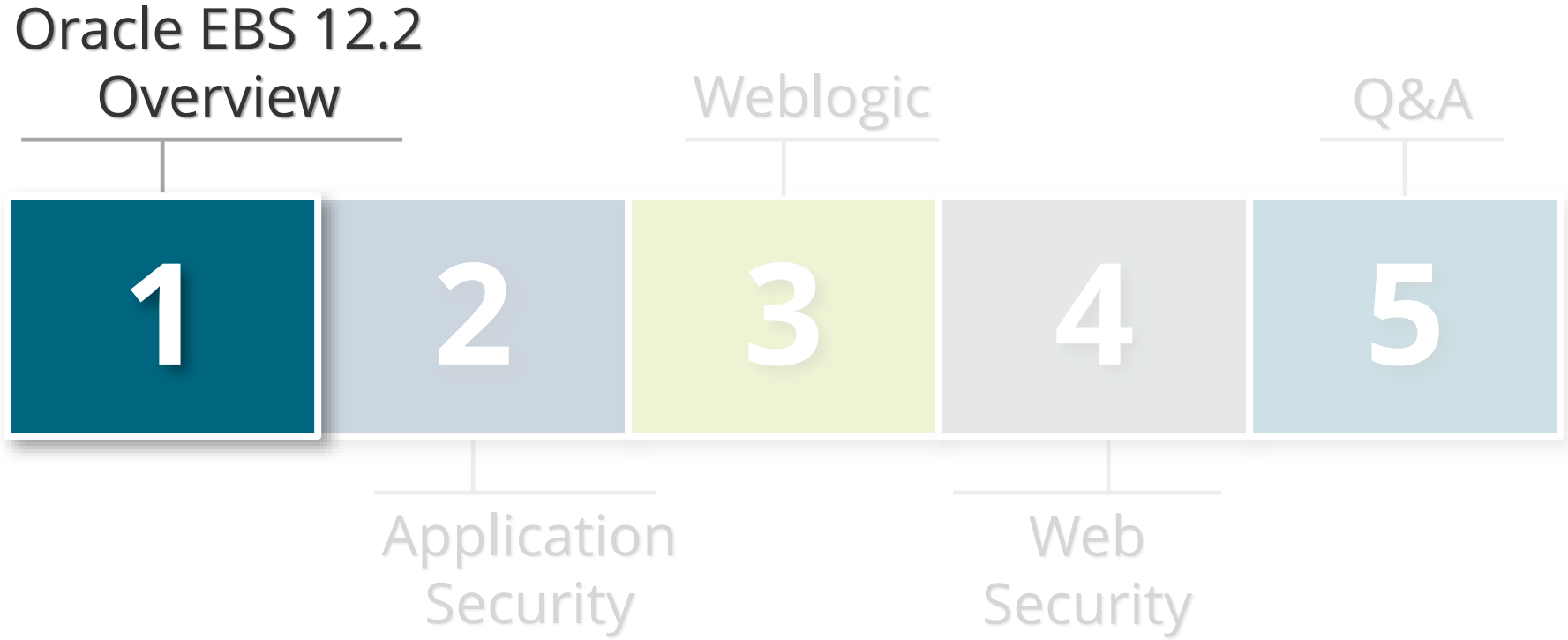
About Integrigy



Agenda

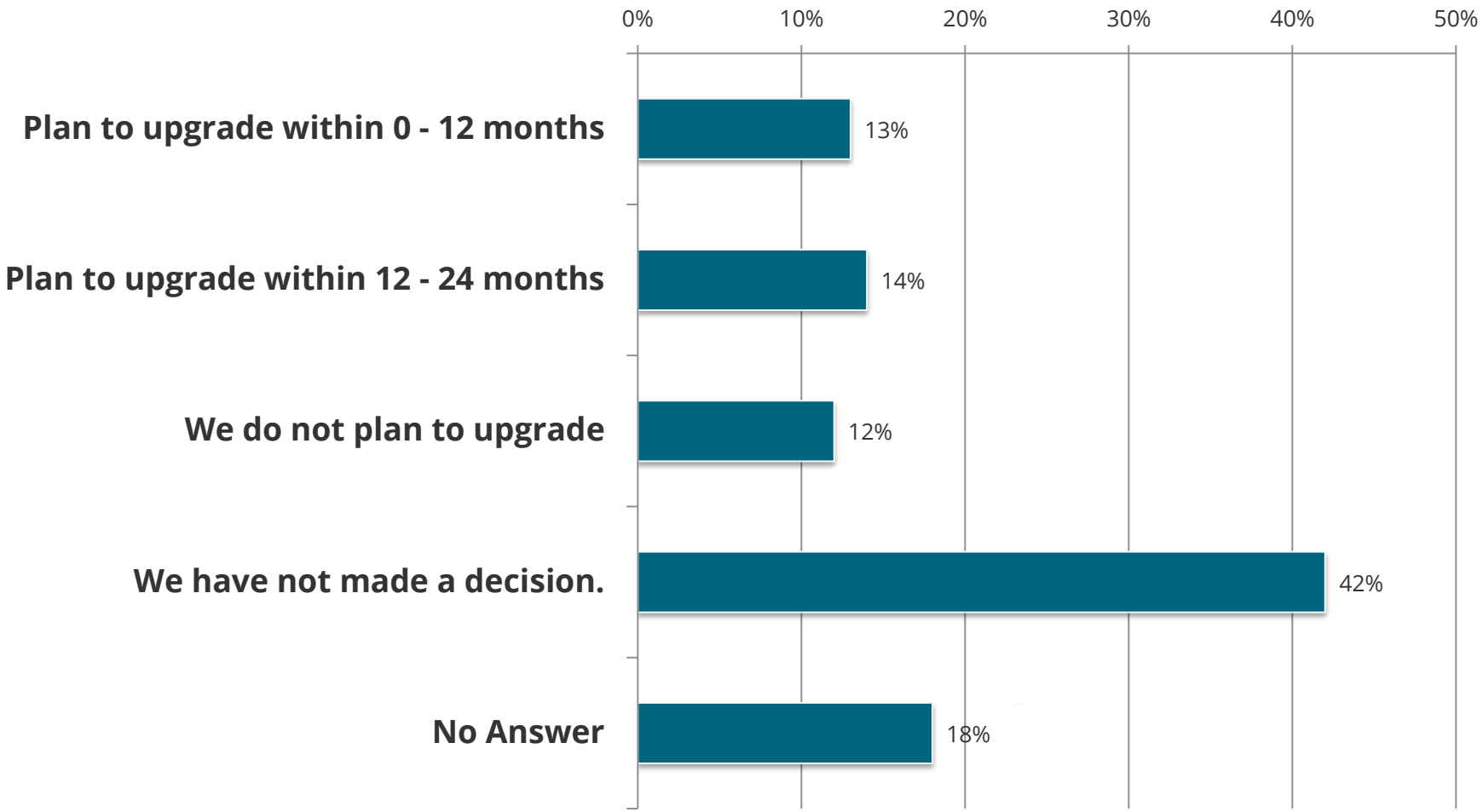

Oracle EBS 12.2
Overview
WebLogic
Q&A
1
2
3
4
5
Application
Security
Web
Security

Agenda

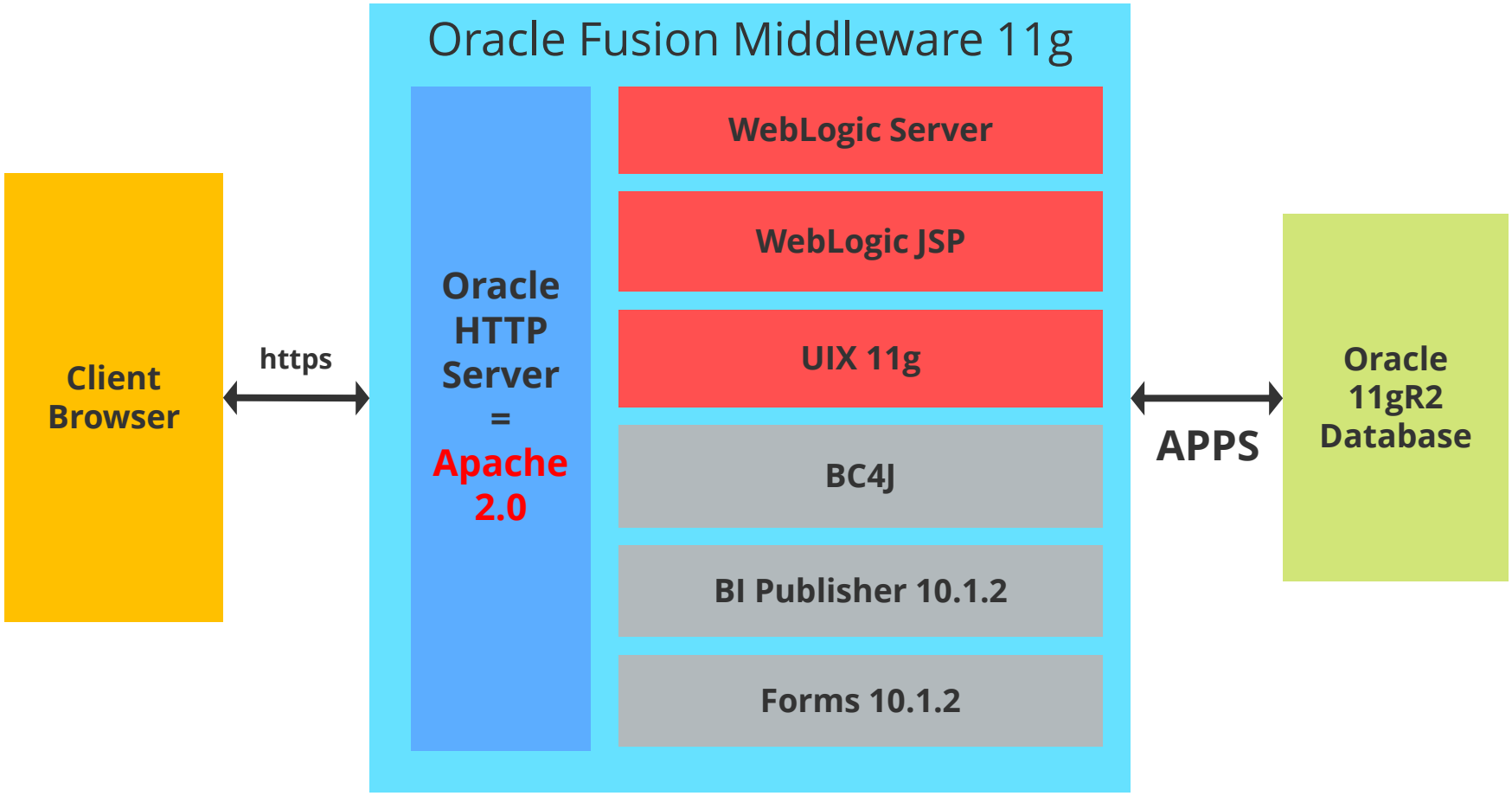

Oracle EBS 12.2 Overview
Weblogic
Q&A
1
2
3
4
5
Application Security
Web Security

Plans to Upgrade to 12.2?

What is your organization's position on upgrading to R12.2?



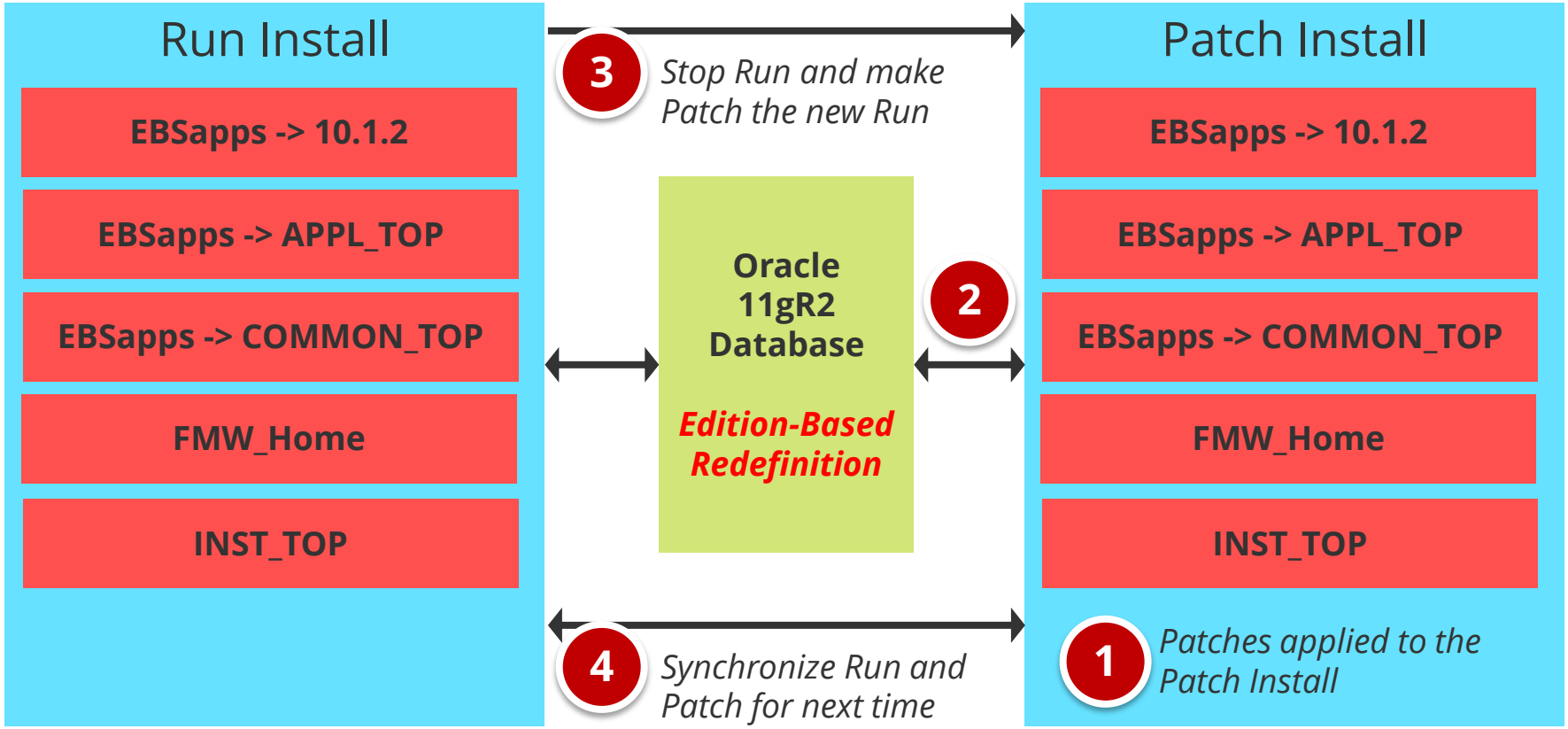
Oracle 12.2 Architecture – Simplified



In 12.2, Oracle Application Server 10g is replaced with Oracle Fusion Middleware 11g, which includes WebLogic Server. All control and management is done using the Oracle Fusion Middleware control.

12.2 Online Patching

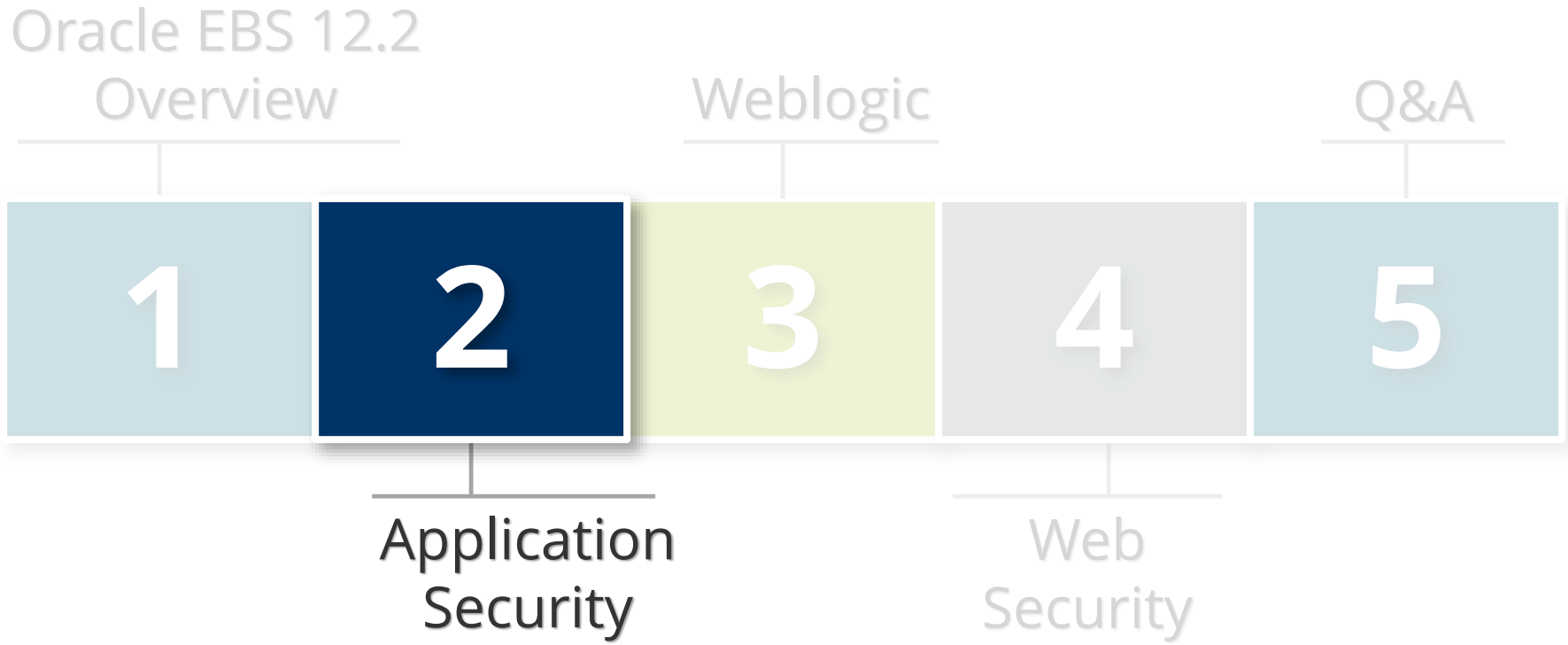
Oracle E-Business Suite 12.2 environment has become much more complex with on-line patching. Database uses Edition-Based Redefinition and two full installs of the application server stack.



12.2 AutoConfig Impact

Configuration Changes	Fusion Middleware Control	WLS Administration Console	Oracle Application Manager & Autoconfig
Database Home			✓ SID name, Listener, dbPorts, etc
Oracle HTTP Server	✓ Performance directives, log configuration, ports, mod_perl, mod_wl_ohs, etc.		
WebLogic Server		✓ oacore, oafm, forms and forms-c4ws services	✓ Classpath and JVM arguments for oacore
E-Business Suite			✓ Concurrent Processing, Profile Options, Developer 10g, Product Specific Settings

Agenda

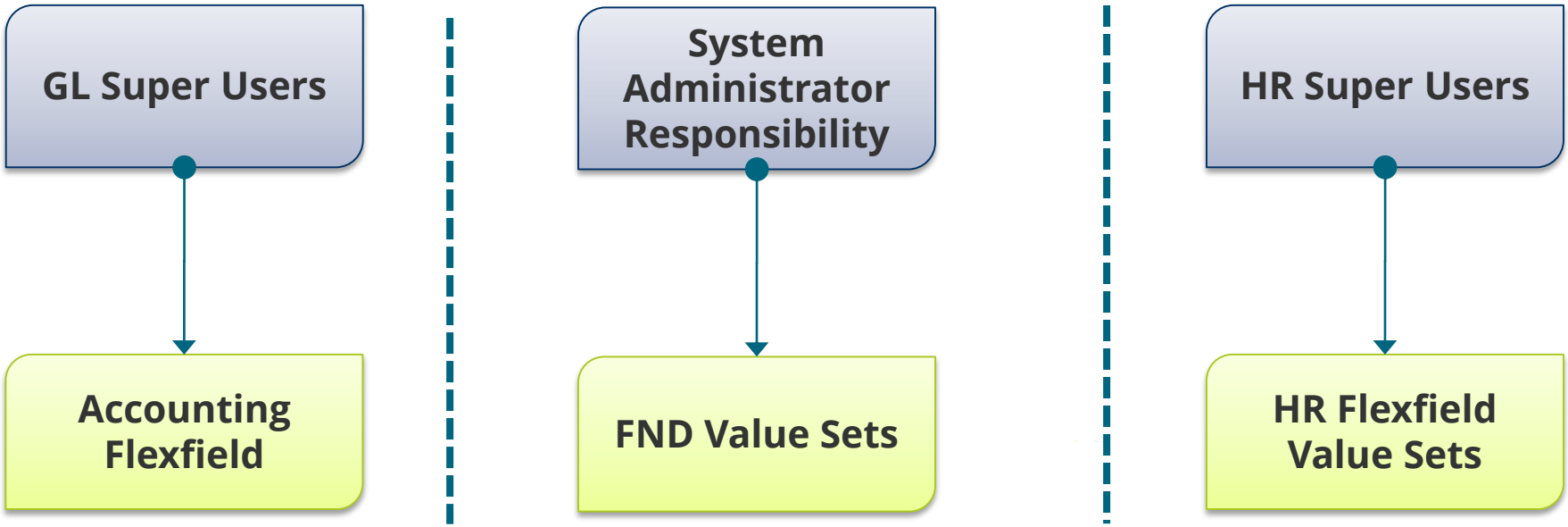

Oracle EBS 12.2
Overview
Weblogic
Q&A
1
2
3
4
5
Application
Security
Web
Security

Flexfield Value Set Security

- **Who can view, insert, or update values for a particular value set in the Segment Values form**
  - Adds segregation of duties to maintenance of flexfield value sets
  - Enabled by default
  - Access must be explicitly granted
  - Access can be based on user, responsibility, role, application, or operating unit

Flexfield Value Set Security Example

Improve segregation of duties by allowing (1) certain users to only view or insert values for Account Flexfields and no other value sets, (2) certain users to only view or insert values for any HR application, and (3) certain users to only view or insert values for a specific operating unit. Roles and responsibilities are also supported.

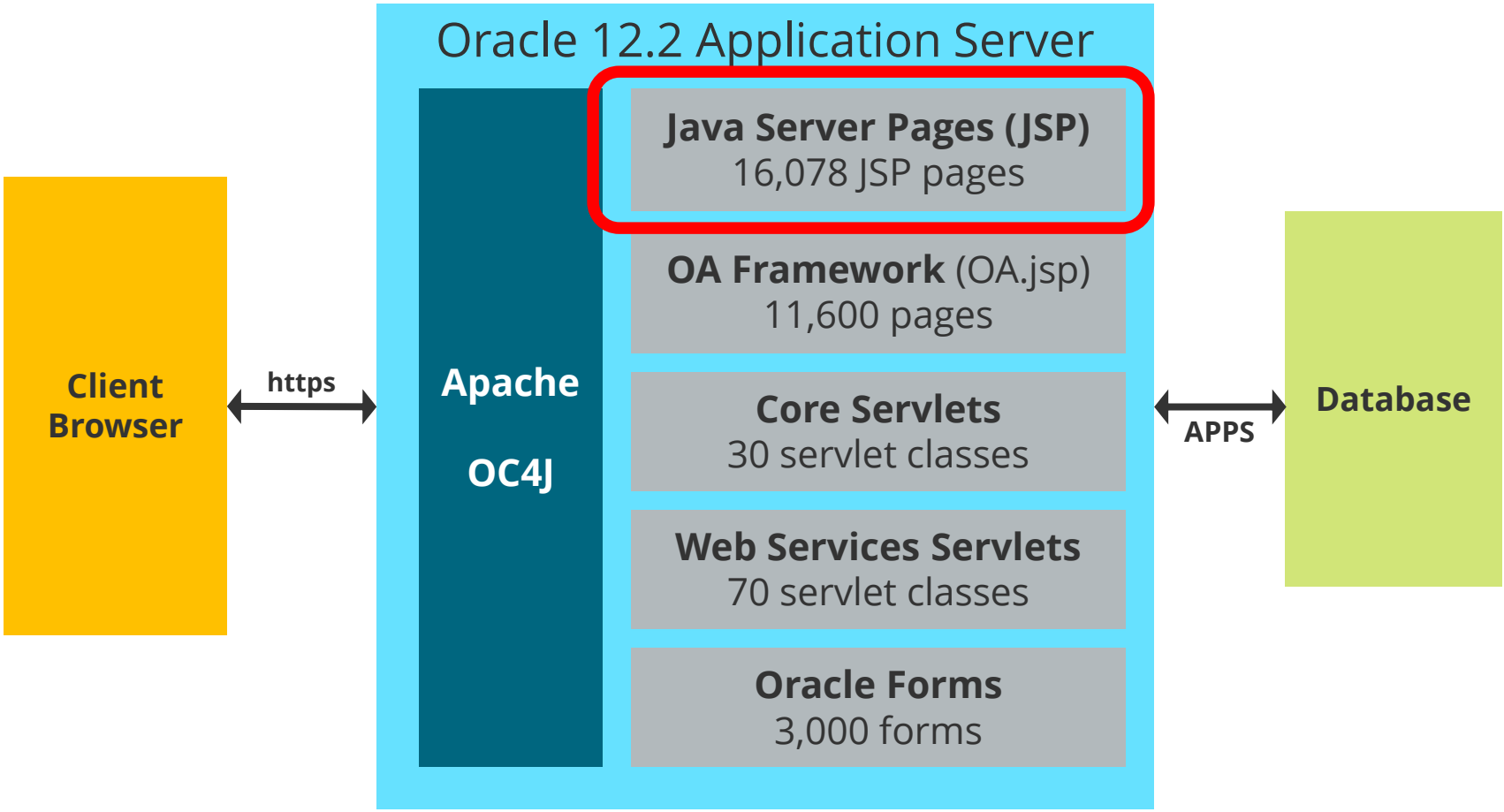


Flexfield Value Set Security

- **Additional Patches Required**
  - Requires the mandatory Patch 17305947:R12.FND.C
- **Additional Setup Required**
  - All values sets locked upon install or upgrade until setup completed
  - *Release 12.2 Flexfield Value Set Security Documentation Update for Patch 17305947:R12.FND.C* (MOS Note ID 1589204.1)
  - MOS Note supersedes 12.2 Flexfields Guide

Allowed JSP Lists

A whitelist of allowed JSP pages. Basically is DMZ URL Firewall for internal access.



Allowed JSP Lists

- Explicit list of allowed JSP pages
- Limits access to unused JSP pages for modules not configured or licensed
- Must be manually enabled
- See the Oracle EBS Security Guide manual for instructions on usage

Allowed JSP Lists

- **Allowed JSP Lists disabled by default**
- **New profile option to allow for disabling of Allow JSP Lists**

Profile Option Name	Description
Allow Unrestricted JSP Access (FND_SEC_ALLOW_JSP_UNRESTRICTED_ACCESS)	Set at Site or Server Level **Yes** – Allow all JSPs **(default)** **No** – Use Allowed JSP Lists

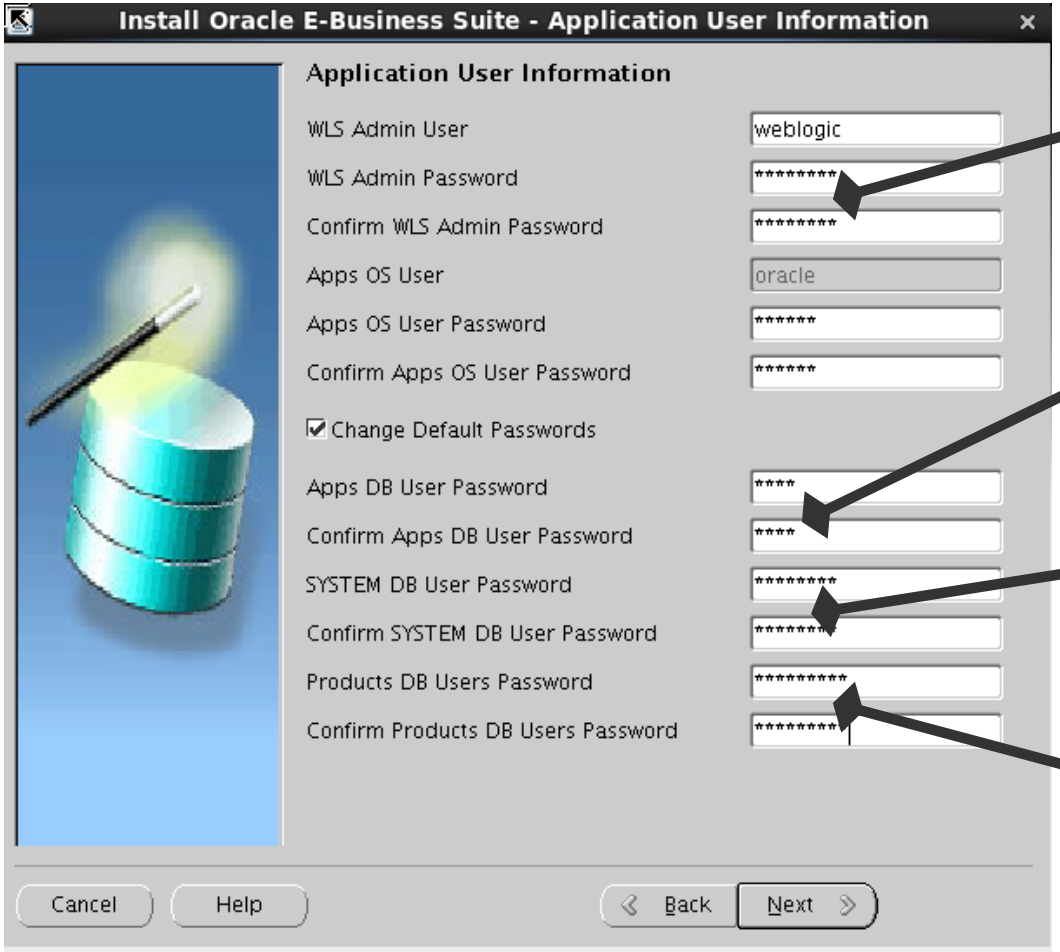
allowed_jsps.conf

```
# $Header: allowed_jsps.conf
120.0.12020000.3 2013/06/11 21:37:29
srveerar noship $
/OA_HTML/AppsLocalLogin.jsp
/OA_HTML/cabo/jsps/a.jsp
/OA_HTML/cabo/jsps/frameRedirect.jsp
/OA_HTML/fndgfm.jsp
/OA_HTML/jsp/fnd/close.jsp
/OA_HTML/jsp/fnd/fnderror.jsp
/OA_HTML/OADownload.jsp
/OA_HTML/OAErrorDetailPage.jsp
/OA_HTML/OAErrorPage.jsp
/OA_HTML/OAExport.jsp
/OA_HTML/OA.jsp
/OA_HTML/OALogout.jsp
/OA_HTML/OARegion.jsp
/OA_HTML/RF.jsp
/OA_HTML/GWY.jsp
/OA_HTML/runforms.jsp
/OA_HTML/xdo_doc_display.jsp
/OA_HTML/OAD.jsp
/OA_HTML/OAP.jsp

include allowed_jsps_FIN.conf
include allowed_jsps_HR.conf
include allowed_jsps_Leasing.conf
include allowed_jsps_Procurement.conf
include allowed_jsps_SCM.conf
include allowed_jsps_CRM.conf
include allowed_jsps_VCP.conf
include allowed_jsps_diag_tests.conf
```

Default Passwords – Fresh Install

Of 191 database accounts, only default password is APPLSYSPUB/PUB



Sets Weblogic control password

Sets APPS and APPLSYS passwords

Sets SYS, SYSTEM, CTXSYS, OUTLN, and 9 other standard database account passwords

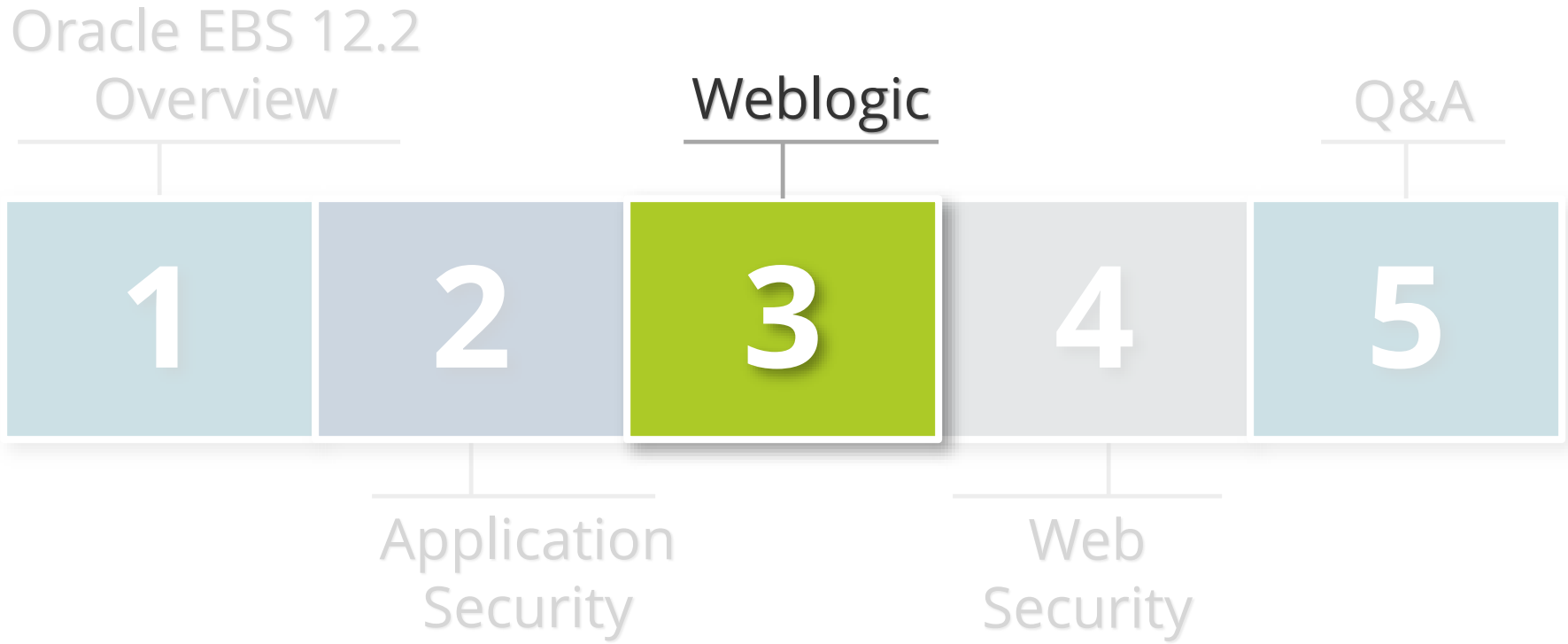
Sets accounts for all EBS product schemas – 161 total accounts

Default Passwords – Upgrade

New database accounts will be added during the database upgrade for new application modules based on from what version you are upgrading from. Be sure to check these accounts for default passwords.

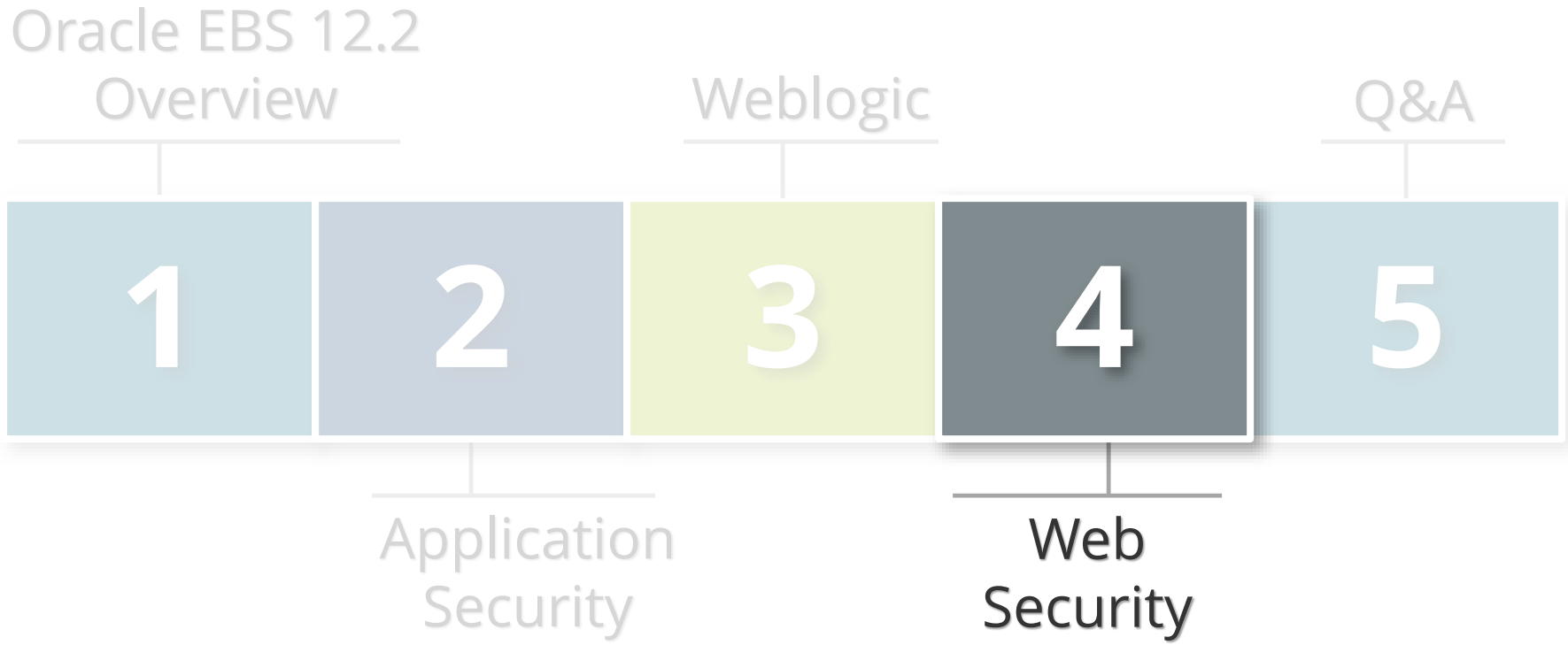
Version Upgrade From	New Database Accounts
11.5.10	XLE ASN FUN FPA ZX LNS IA XDO
12.0.0	JMF GMO IBW IPM DNA
12.0.4	IZU
12.1.0	RRS DPP MTH QPR DDR INL
12.2.2	GHG APPS_NE

Agenda


Oracle EBS 12.2
Overview
Weblogic
Q&A
1
2
3
4
5
Application
Security
Web
Security

WebLogic/Fusion Middleware Control Demonstration

Agenda


Oracle EBS 12.2 Overview
Weblogic
Q&A
1
2
3
4
5
Application Security
Web Security

Clickjacking Protection

- **Frame Busting**
  - Provides protection against clickjacking by disallowing OA Framework pages from being embedded into frames from third-party sites
  - Enabled by default

Profile Option Name	Description
FND: Disable Frame Busting (FND_DISABLE_FRAME_BUSTING)	Set at Site or Server Level **True** – Disable frame busting **False** – Use frame busting **(default)**

Clickjacking Protection

X-Frame-Options HTTP response header

- Now enabled for all Oracle EBS web pages and configured in the Apache httpd.conf
- Enabled by default

Attachment Virus Scanning

- **Enhanced virus scanning of all attachments and file uploads**
  - Limited to Symantec server
  - Can be enabled or disabled at site, responsibility, application or user level with **FND: Disable Virus Scan**
  - OA Framework customizations can selectively enable or disable virus scanning
  - Virus scanning should be utilized when implementing iRecruitment or iSupplier

Additional Web Application Security

- **Cookie Domains**
  - Protects the Oracle EBS session cookie from web-based attacks
  - Set to domain by default in profile option ICX_SESSION_COOKIE_DOMAIN

- **Cross-site Scripting (XSS) Protections**
  - Check file uploads and attachments for XSS
  - XSS checking in Messaging Rich Text Editor
  - Use AntiSamy library for XSS filtering

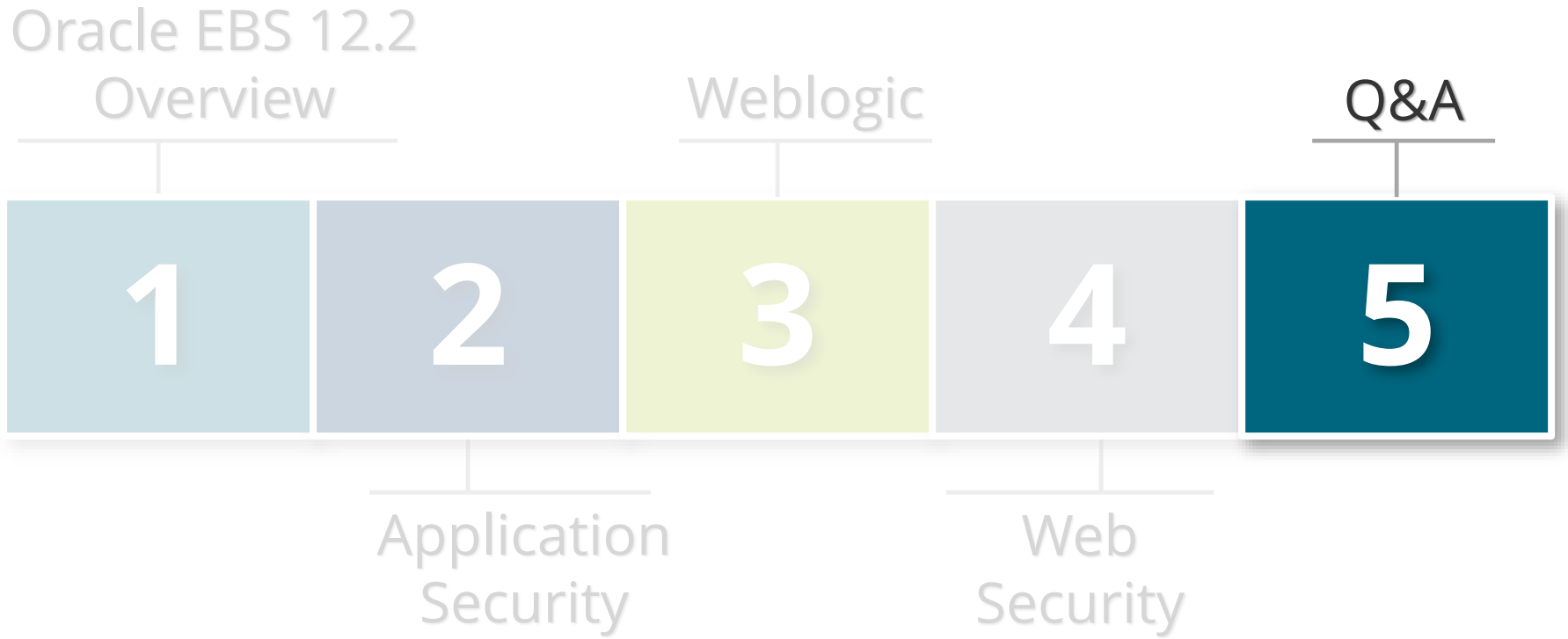
Security Concerns

- **Delivery Manager report output**
  - Send reports to EBS users through e-mail
  - Upload reports to an FTP server
  - Save reports to the local file system of the EBS application tier
- **SOA and Web Services (REST)**
  - Do your DBA and security teams understand web services and how to properly secure them?

Security Concerns

- **Encrypted vs. Non-Reversible Hashed Application Passwords**
  - Default for EBS application accounts is still encrypted passwords vs. non-reversible hashed passwords

Agenda


Oracle EBS 12.2 Overview
Weblogic
Q&A
1
2
3
4
5
Application Security
Web Security

References

- Database Initialization Parameters for Oracle E-Business Suite Release 12 (Doc ID 396009.1)
- Oracle E-Business Suite Product Specific Release Notes, Release 12.2.2 (Doc ID 1585844.1)
- Oracle Application Framework Profile Options Release 12.2 (Doc ID 1373537.1)

Contact Information

Stephen Kost

Chief Technology Officer

Integrigy Corporation

web: **www.integrigy.com**

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

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

youtube: **youtube.com/integrigy**