Common Mistakes When Deploying Oracle E-Business Suite to the Internet

February 9, 2017

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

About Integrigy

ERP Applications
Oracle E-Business Suite,
PeopleSoft, Oracle Retail

INTEGRIGY

Databases
Oracle, Microsoft SQL Server,
DB2, Sybase, 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
ERP, Database, Sensitive Data, Pen Testing

Ensure Compliance

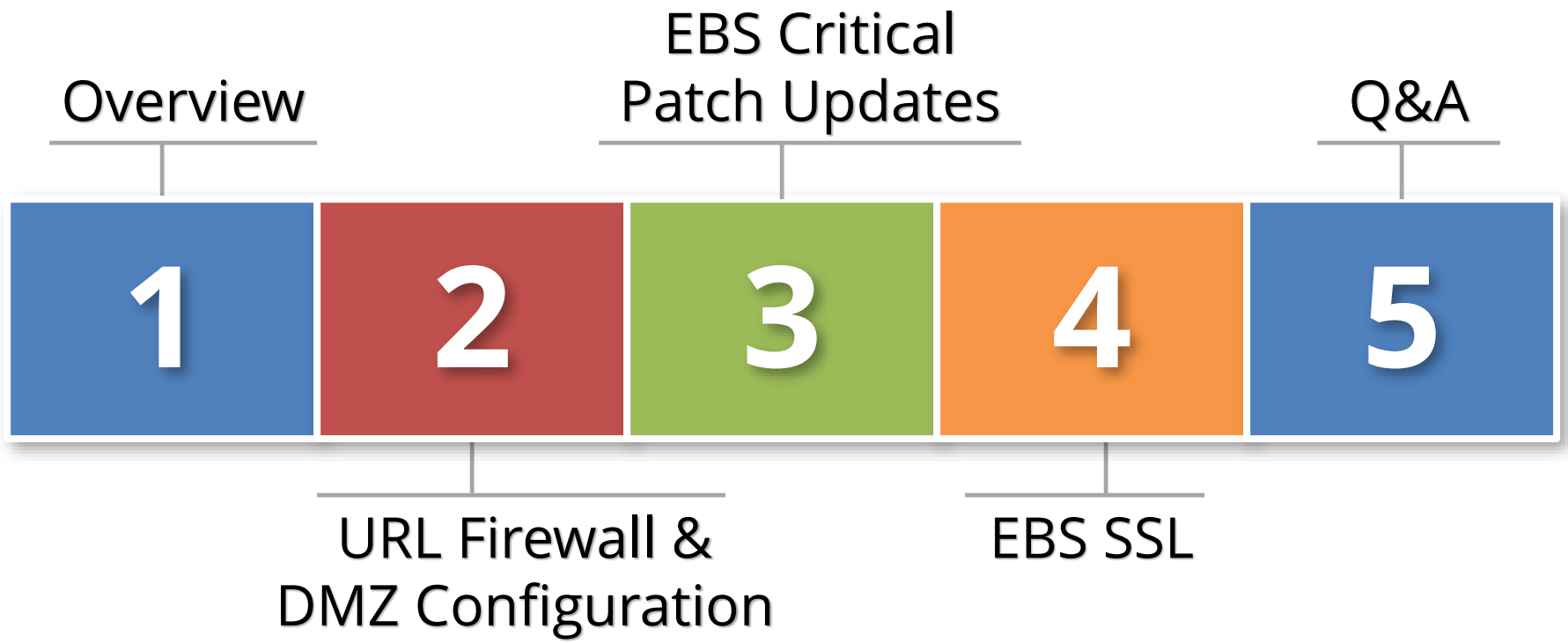
Compliance Assistance
SOX, PCI, HIPAA, GLBA

Build Security

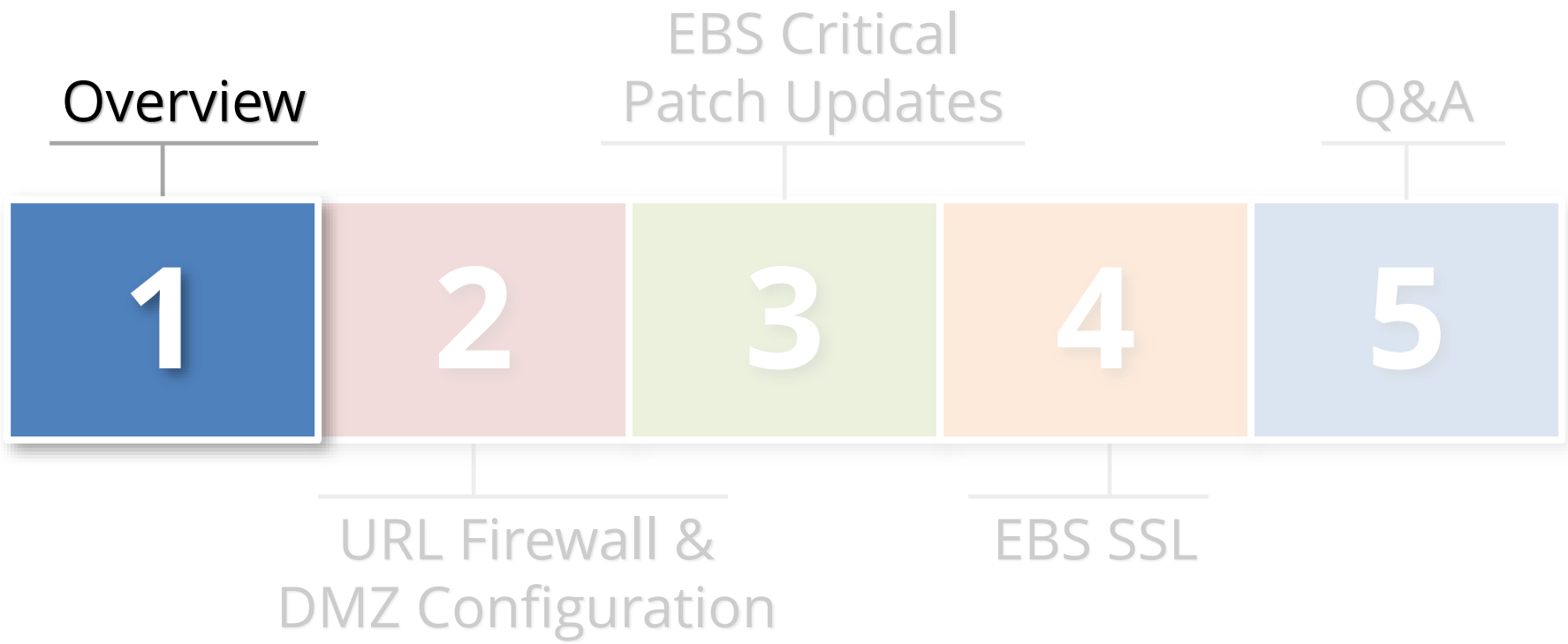
Security Design Services
Auditing, Encryption, DMZ

Integrigy Research Team
ERP Application and Database Security Research

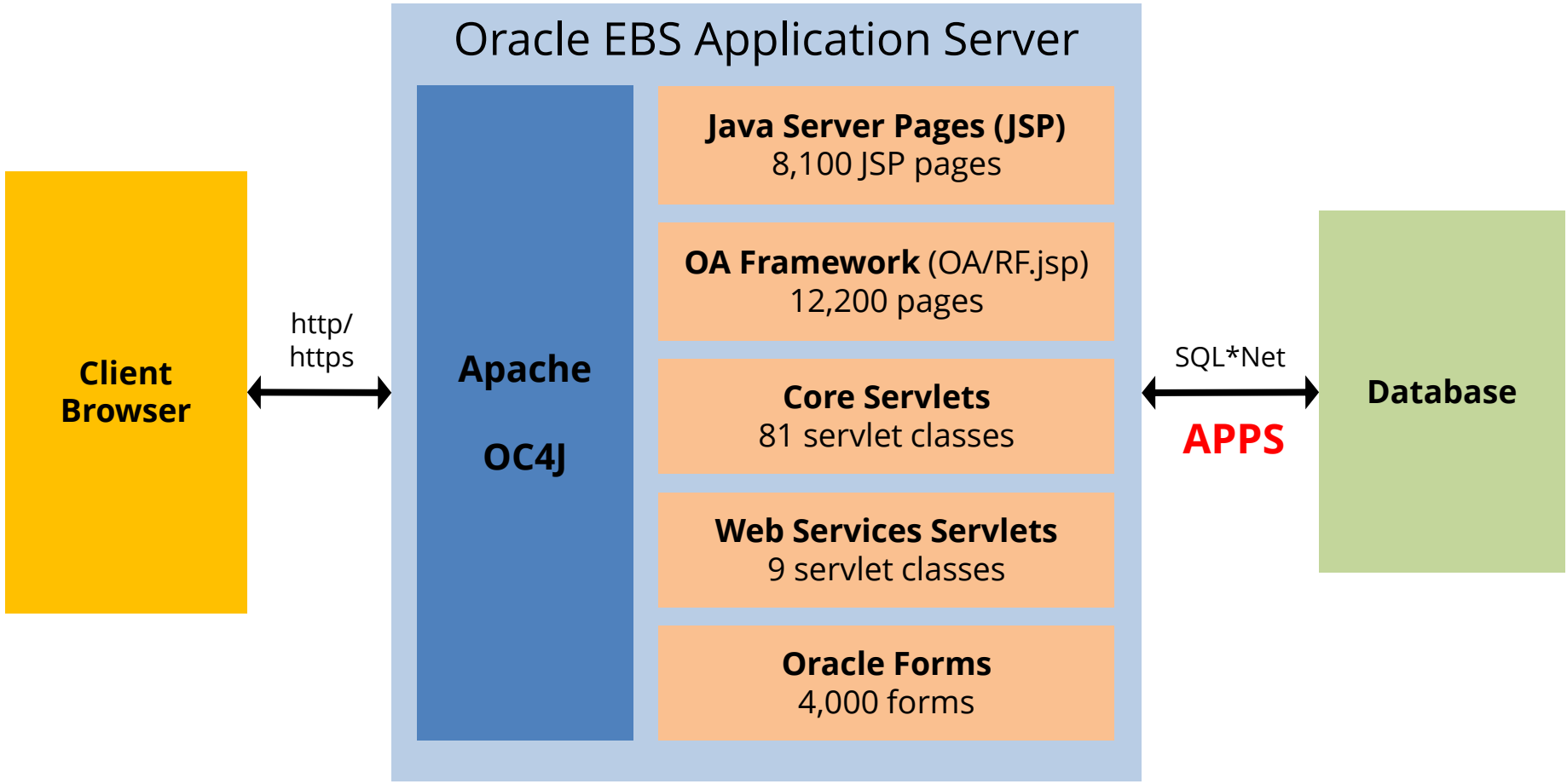
Agenda


Overview
EBS Critical Patch Updates
Q&A
1
2
3
4
5
URL Firewall & DMZ Configuration
EBS SSL

Agenda

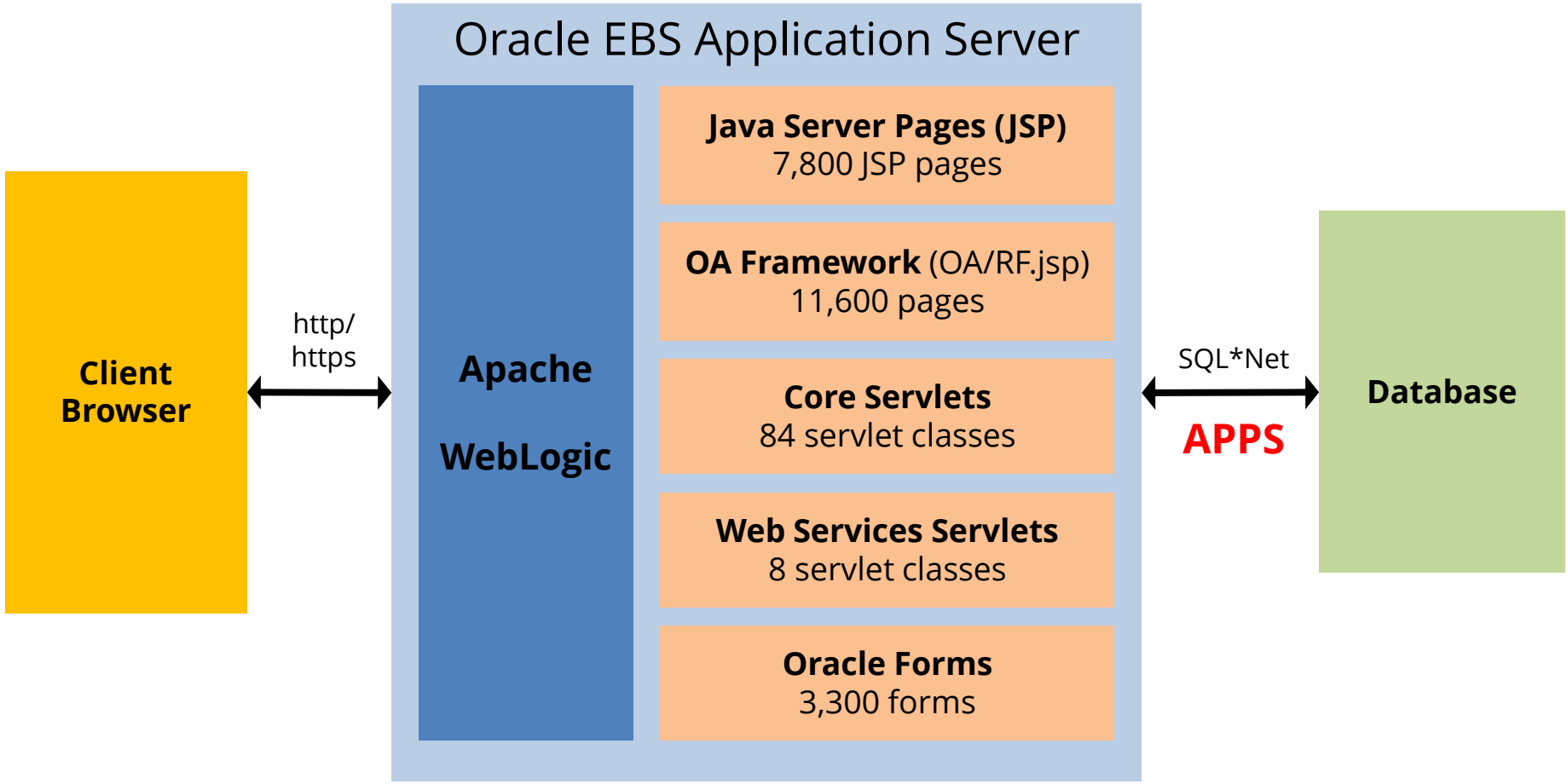

Overview
EBS Critical Patch Updates
Q&A
1
2
3
4
5
URL Firewall & DMZ Configuration
EBS SSL

Oracle EBS 12.0/12.1 DMZ Configuration



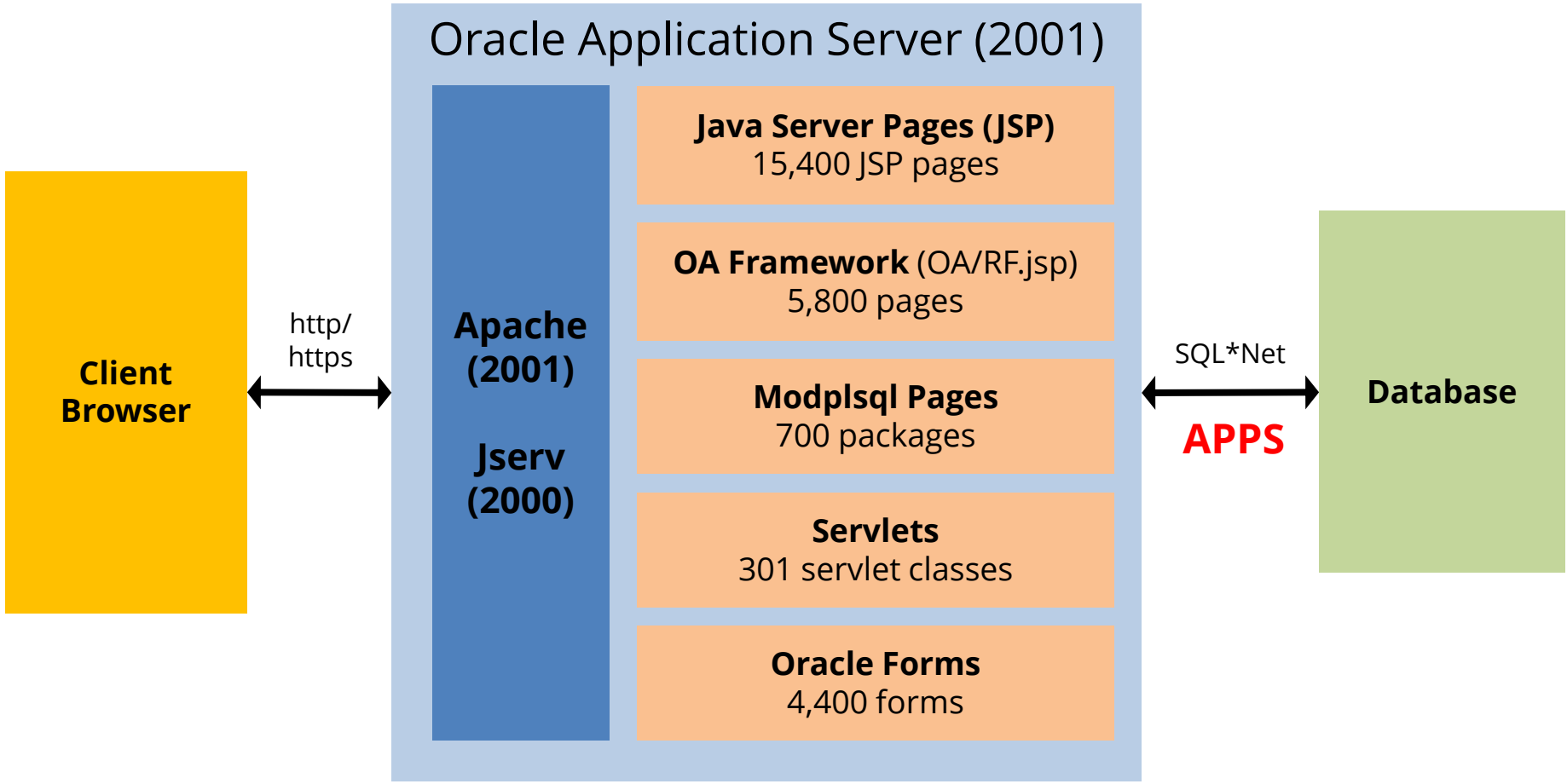
All Oracle E-Business Suite environments include **ALL modules (250+) and ALL web pages (20,000+)** even if modules are not installed, licensed, or configured. Many security vulnerabilities exist in unused modules.

Oracle EBS 12.2 DMZ Configuration



All Oracle E-Business Suite environments include **ALL modules (250+) and ALL web pages (20,000+)** even if modules are not installed, licensed, or configured. Many security vulnerabilities exist in unused modules.

Oracle EBS 11i DMZ Configuration



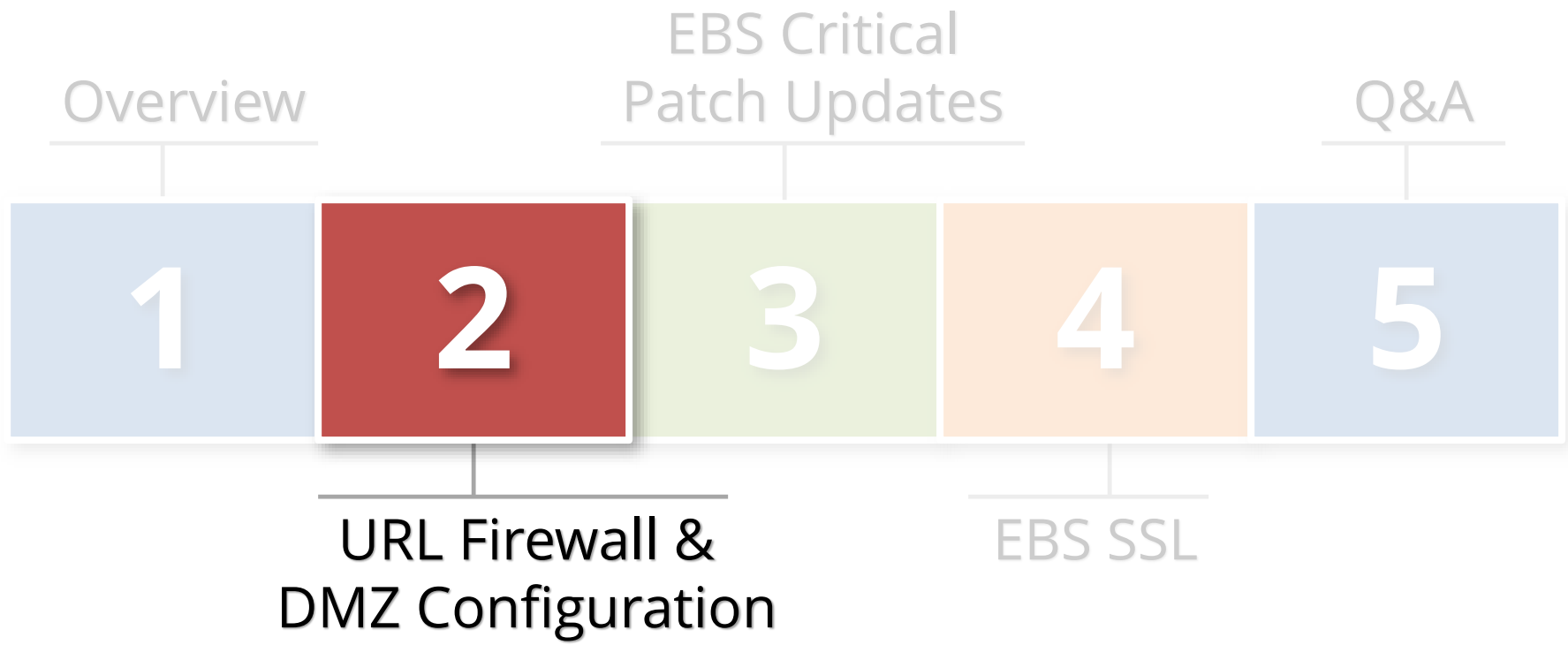
All Oracle E-Business Suite environments include **ALL modules (250+) and ALL web pages (20,000+)** even if modules are not installed, licensed, or configured. Many security vulnerabilities exist in unused modules.

Oracle EBS 11i Web Components

Component	11i Version	Release Date	Non-EBS Desupport[1]
Oracle Application Server[3]	1.0.2.2.2	Dec 2001	June 2004
Apache[3]	1.3.9	Feb 2001	Feb 2010
Jserv	1.1.2	June 2000	June 2006
mod_security	1.8.4	July 2004	May 2006
OpenSSL	0.9.5a	Sept 2000	March 2004
	0.9.8zh[2]	Dec 2015	Dec 2016

1. Oracle EBS 11i web components are desupported but had support exceptions for 11i environments through January 2016. As of January 2016, all support for 11i and associated technology stack components has ended.
2. OpenSSL updated from 0.9.5a to 0.9.8zh with July 2015 Critical Patch Update for OAS 1.0.2.2.2.
3. Security vulnerabilities are patched but version is not upgraded.

Agenda


Overview
EBS Critical Patch Updates
Q&A
1
2
3
4
5
URL Firewall & DMZ Configuration
EBS SSL

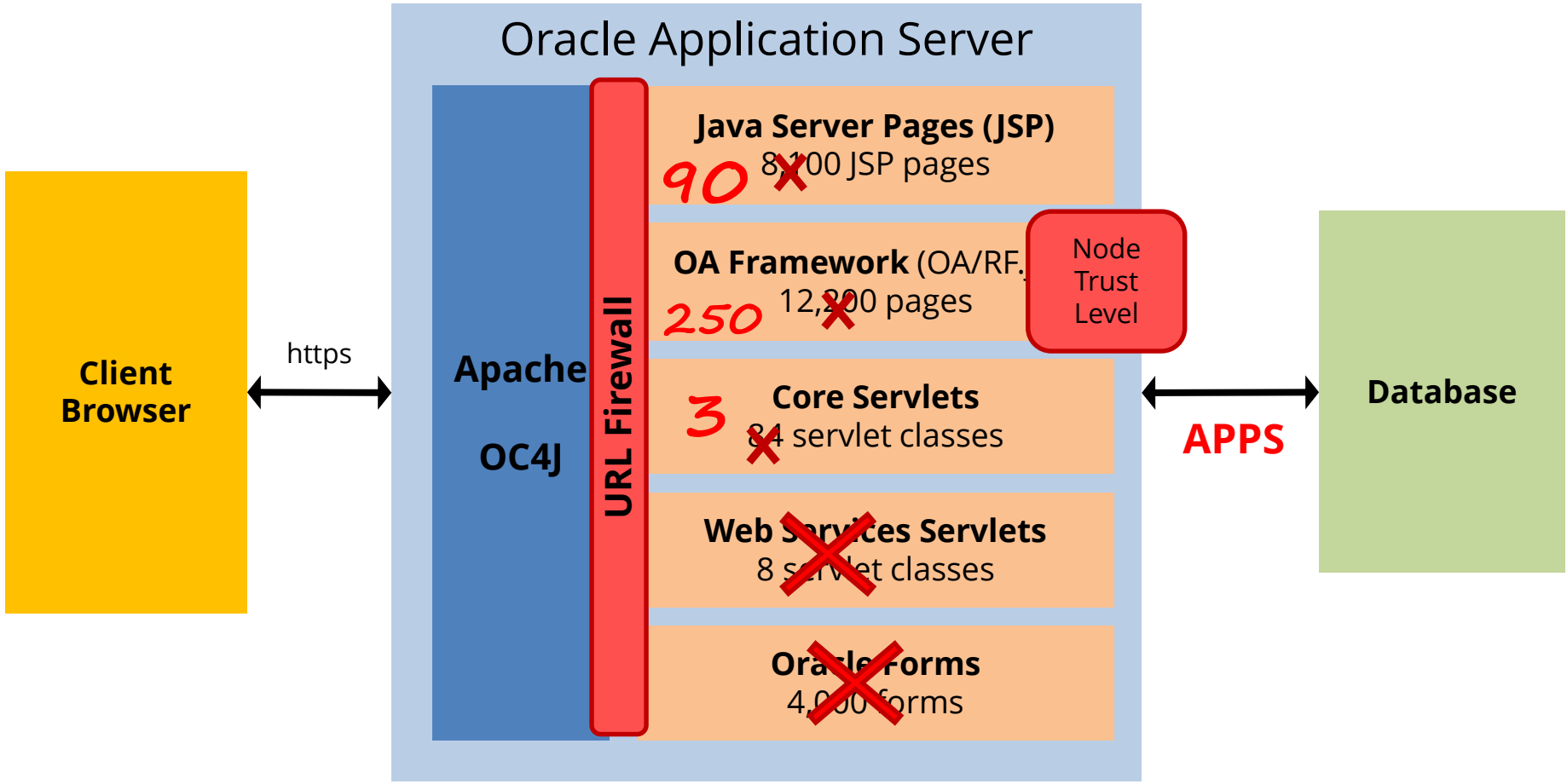
Oracle EBS DMZ MOS Notes

Deploying Oracle E-Business Suite in a de-militarized zone (DMZ) requires a specific and detailed configuration of the application and application server. **All steps must be followed** in the Oracle provided My Oracle Support Note.

“Oracle EBS Configuration in a DMZ”

12.2	1375670.1
12.1/12.0	380490.1
11i	287176.1

Oracle EBS R12 DMZ Configuration



- Proper **DMZ configuration** reduces accessible pages and responsibilities to only those required for external access. Reducing the application surface area eliminates possible exploiting of vulnerabilities in non-external modules. (See MOS Note ID 380490.1)

Oracle EBS DMZ Certified Modules (R12)

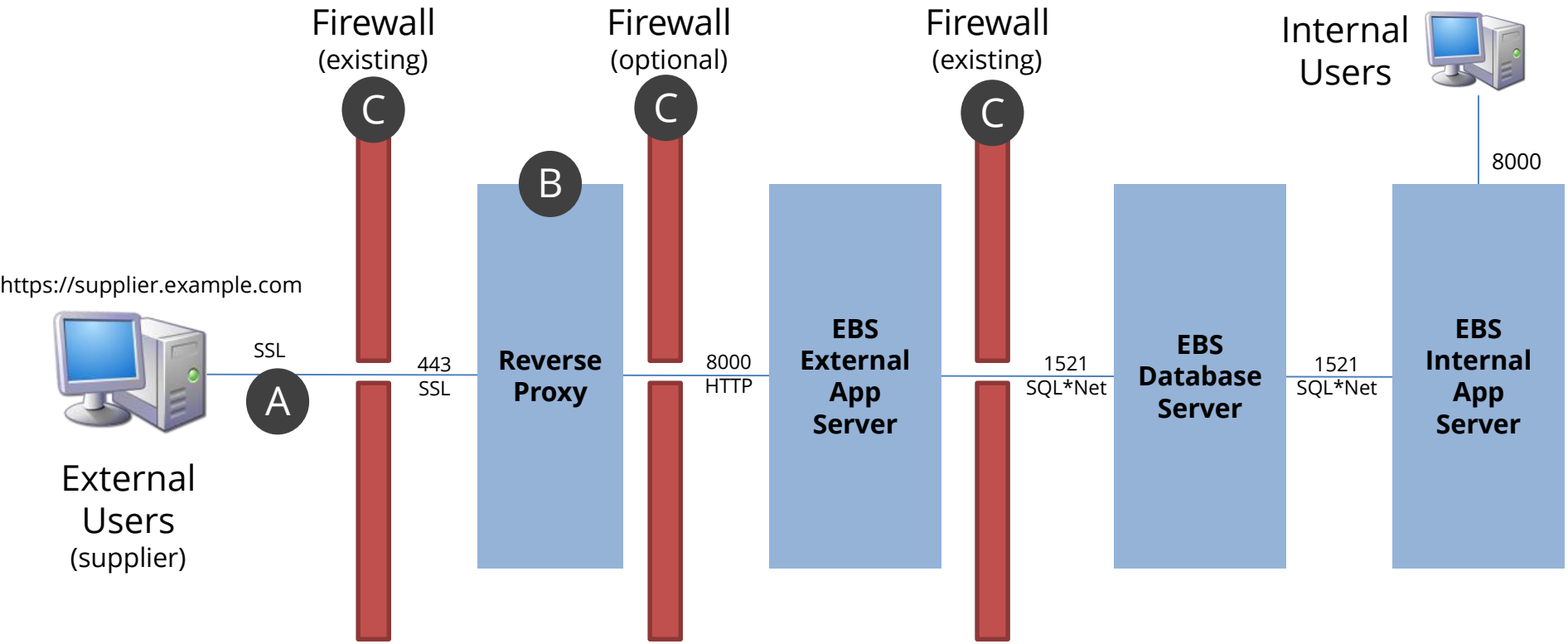
Oracle only certifies a limited set of modules for use in a DMZ

- Meets DMZ architectural requirements (i.e., no forms)
- URL Firewall rules provided for the module

iSupplier Portal (POS)
Oracle Sourcing (PON)
Oracle Receivables (OIR)
iRecruitment (IRC)
Oracle Time and Labor (OTL)
Oracle Learning Management (OTA)
Self Service Benefits (BEN)
Self Service Human Resources (SSHR)
Oracle iSupport (IBU)
Oracle iStore (IBE)
Oracle Marketing (AMS)
Oracle Partner Relationship Mgmt (PRM)
Oracle Survey (IES)

Oracle Transportation (FTE)
Oracle Contracts Core (OKC)
Oracle Service Contracts (OKS)
Oracle Collaborative Planning (SCE)
Oracle User Management (UMX)
Order Information Portal (ONT)
Oracle Sales for Handhelds (ASP)
Oracle Internet Expenses (OIE)
Oracle Performance Management (OPM)
Compensation Workbench (CWB)
Oracle Payroll (PAY)
Oracle Quoting (QOT)
Oracle Field Service 3rd Party Portal (FSE)

EBS DMZ Architecture

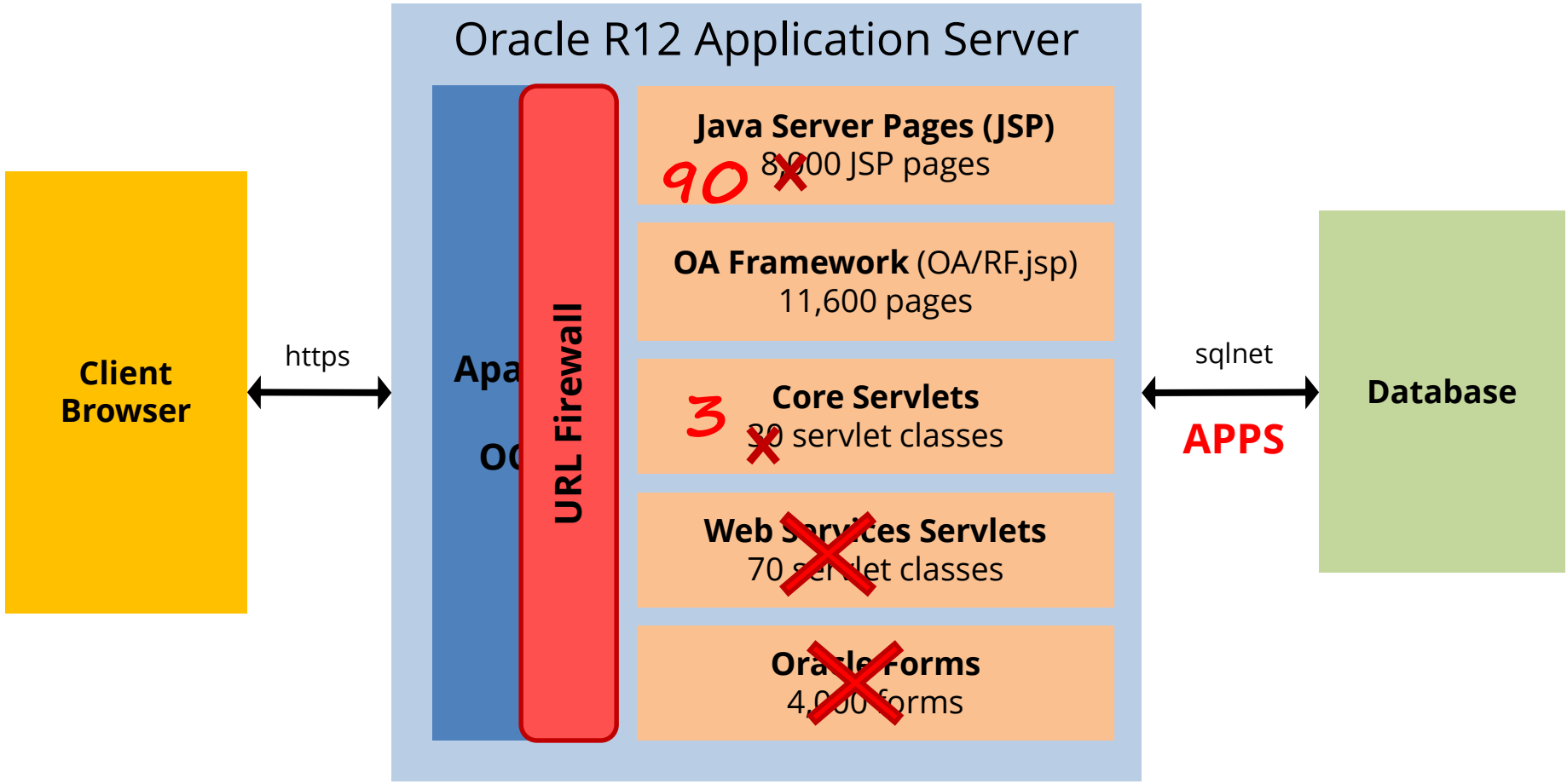


A **HTTPS/SSL** should always be used otherwise passwords and data are sent in the clear.

B A **reverse proxy** server should be implemented such as Apache, Blue Coat, or F5 BIG-IP.

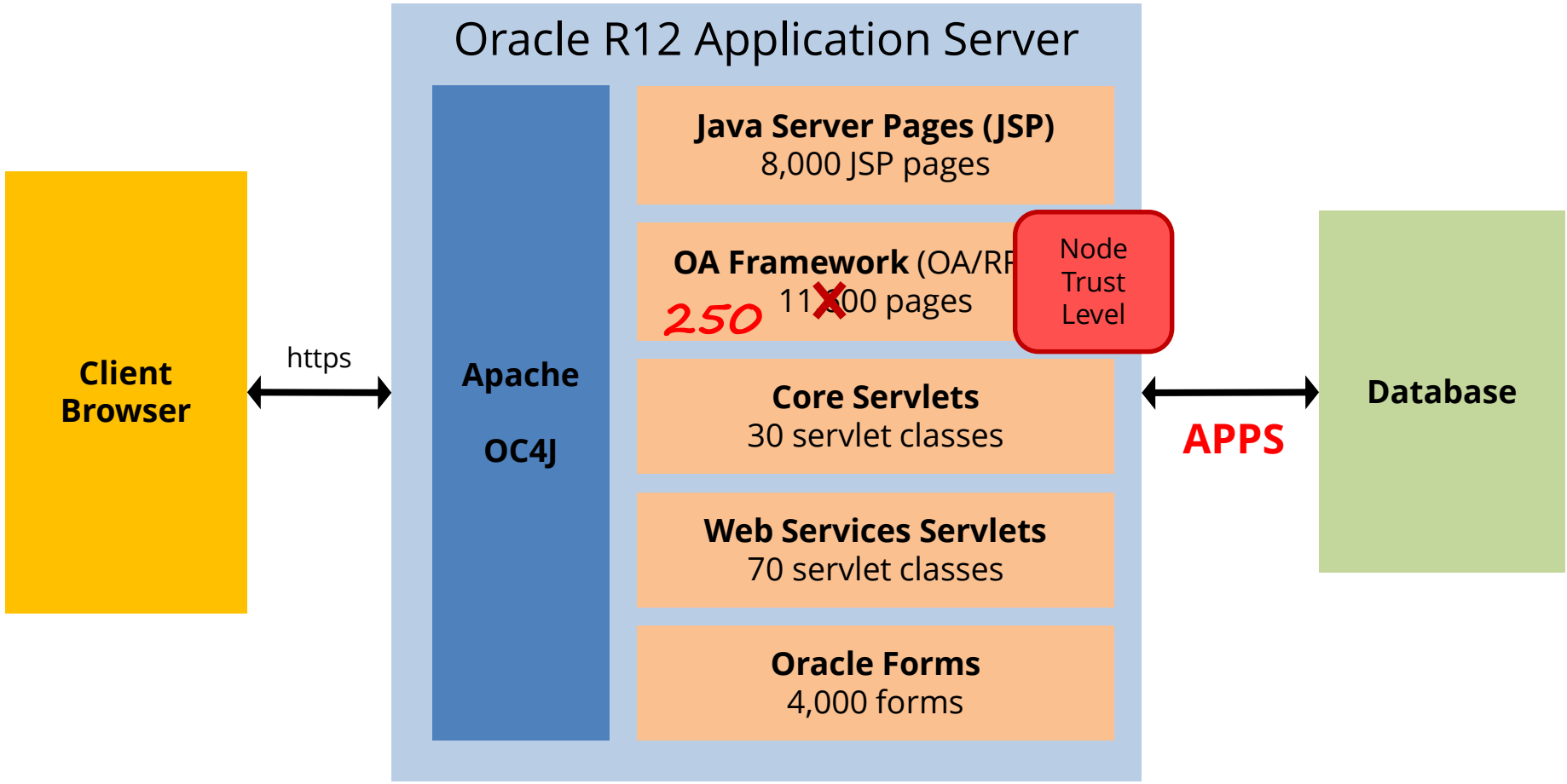
C Firewall between layers block access between layers except for explicitly defined ports.

DMZ Step Appendix E – URL Firewall



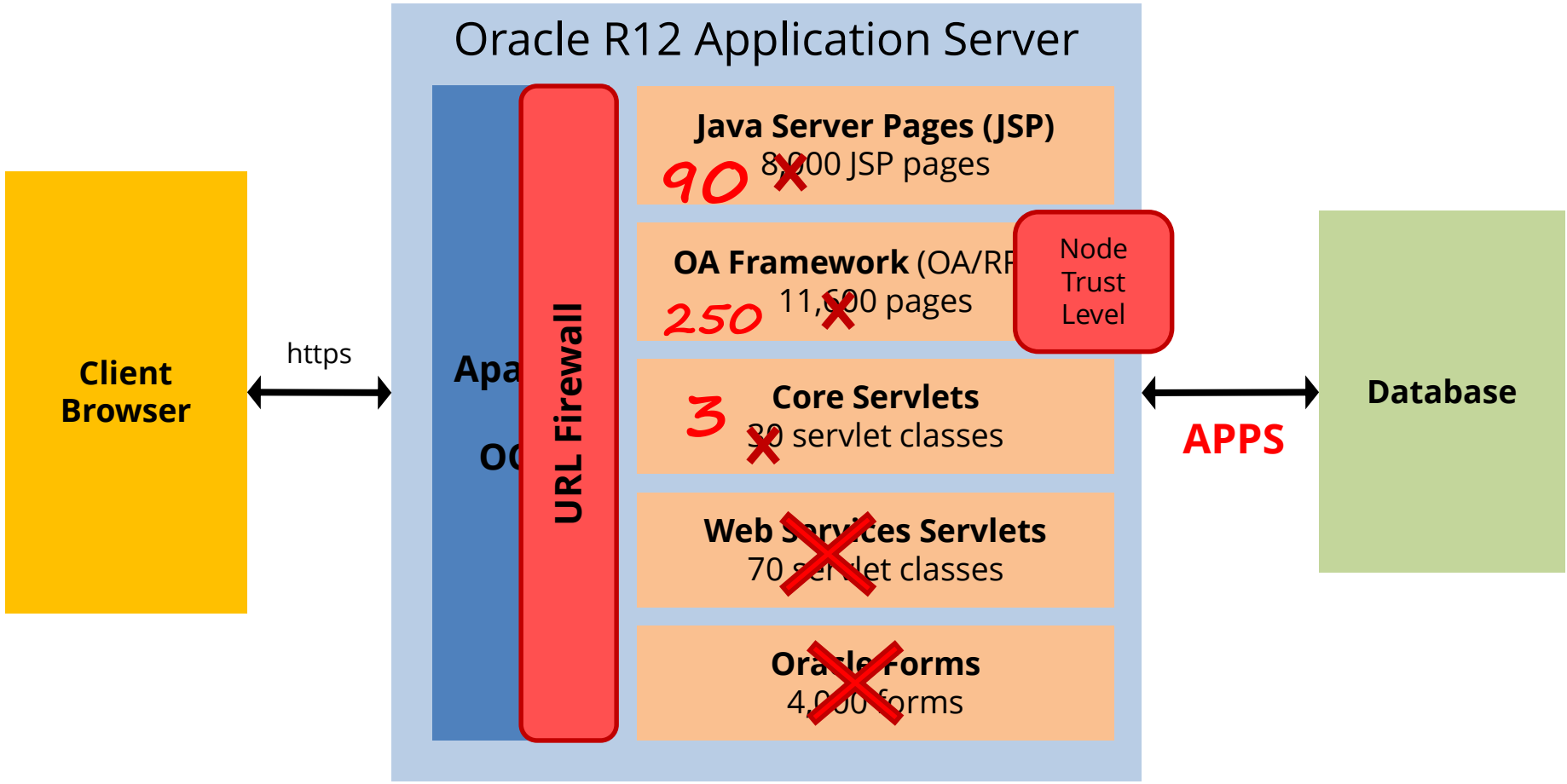
- **URL Firewall** in Appendix E is absolutely mandatory. Configure using **url_fw.conf**.
- A **whitelist** of allowed JSP pages and servlets. Allows all OA Framework pages.

DMZ Steps 5.2 & 5.3 – Responsibilities



- Step 5.2 is set the **NODE_TRUST_LEVEL to EXTERNAL** for the external application server.
- Step 5.3 **limits the responsibilities** accessible via the external application server.

DMZ Configuration

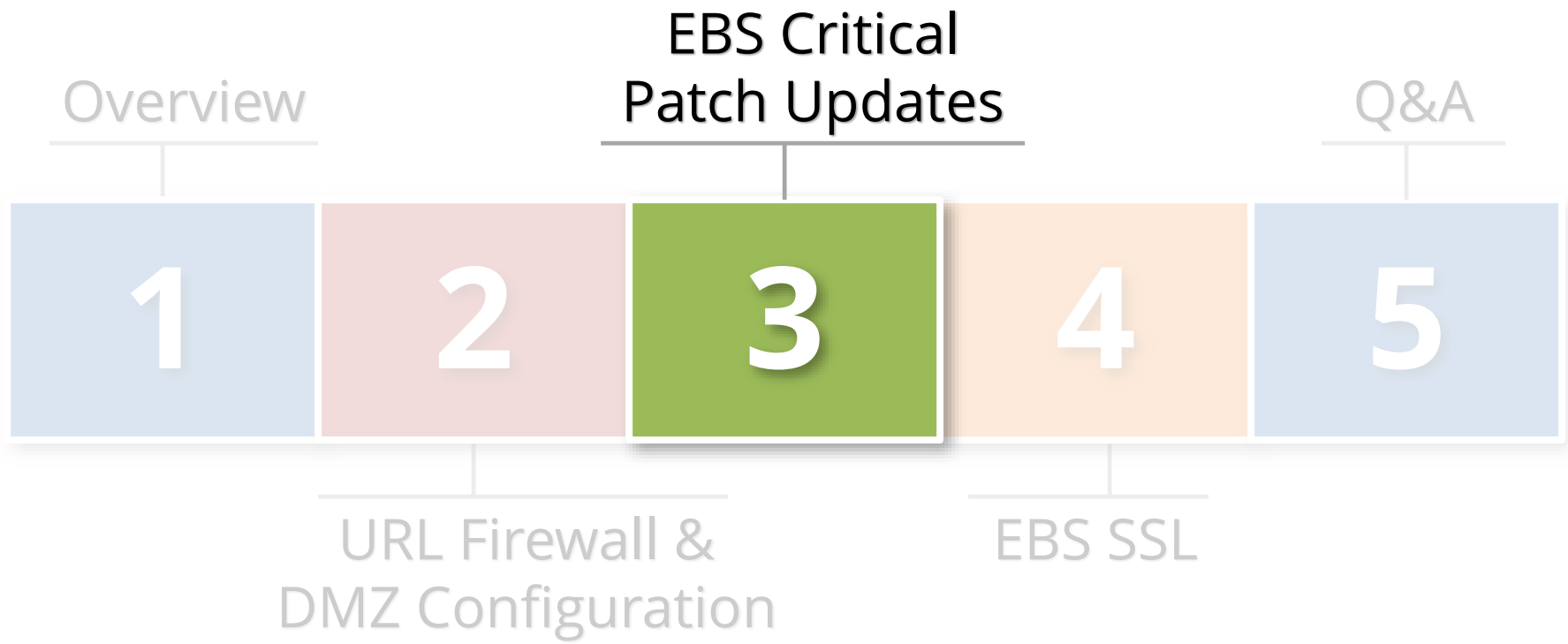


- Proper **DMZ configuration** reduces accessible pages and responsibilities to only those required for external access. Reducing the application surface area eliminates possible exploiting of vulnerabilities in non-external modules.

Common Mistakes

Mistake	Impact	Risk
URL Firewall in Appendix E not enabled or incorrectly enabled	▪ 20,000 EBS web pages exposed on the Internet ▪ Many EBS web pages may have unpatched security vulnerabilities ▪ Diagnostic and debugging may be available	High
EBS DMZ server not marked as external server	▪ URL Firewall and Node Trust Level will not be enabled	High
Node Trust Level includes too many responsibilities	▪ Unnecessary OA Framework web pages exposed on the Internet	Medium
FND_DIAGNOSTICS enabled	▪ Attacker can access significant information on the EBS configuration.	Medium

Agenda


Overview
EBS Critical Patch Updates
Q&A
1
2
3
4
5
URL Firewall & DMZ Configuration
EBS SSL

Oracle EBS Security Vulnerabilities

Oracle E-Business Suite security vulnerabilities fixed between January 2005 and January 2017

581

Oracle EBS Web Vulnerabilities Fixed

~130 SQL Injection in web pages

~220 Cross Site Scripting

~40 Authorization/Authentication

~20 Business Logic Issues

Oracle E-Business Suite Version Support

Version	Premier Support End Date	Extended Support End Date (1)	CPU Support End Date
EBS 12.2	September 2021	TBD	**TBD**
EBS 12.1	December 2016	December 2019	**October 2019**
~~**EBS 12.0**~~	~~January 2012~~	~~January 2015~~	**January 2015**
~~**EBS 11.5.10**~~	~~November 2010~~	~~November 2013~~	**January 2016 (2, 3)** October 2017 (ACS only)
~~**EBS 11.5.9**~~	~~June 2008~~	~~N/A~~	~~July 2008~~
~~**EBS 11.5.8**~~	~~November 2007~~	~~N/A~~	~~October 2007~~
~~**EBS 11.5.7**~~	~~May 2007~~	~~N/A~~	~~April 2007~~

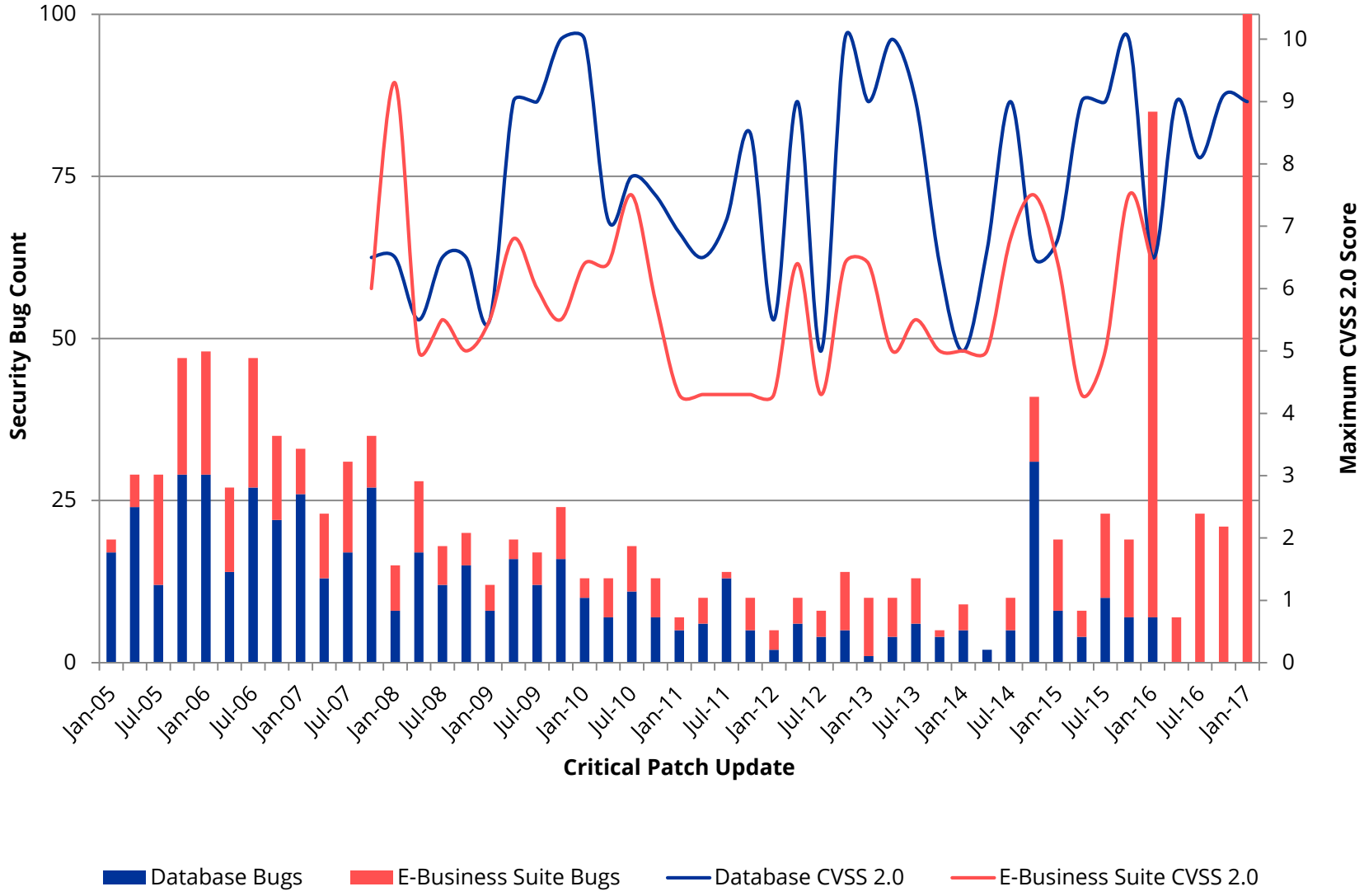
1. Extended support requires a minimum baseline patch level – see MOS Note ID 1195034.1.
2. After January 2016, CPUs are available for customers with Advanced Support Contracts.
3. 11.5.10 Sustaining support exception through January 2016 provided CPUs.

Oracle EBS Extended Support Requirements

12.2	▪ EBS 12.2.3 ▪ R12.AD.C.DELTA.7
12.1	▪ Basically 12.1.3 ▪ Application Server 10.1.3.5
12.0	▪ EBS 12.0.6 ▪ Application Server 10.1.2.3 & 10.1.3.5 ▪ Java 6
11.5.10	▪ ATG RUP 6 or ATG RUP 7

Source: MOS Note ID 1195034.1 - Oracle E-Business Suite Error Correction Support Policy (V.5 – January 2015)

Oracle Security Vulnerabilities per Quarter



Oracle EBS CPU Risks and Threats

The risk of Oracle E-Business Suite security vulnerabilities depends if the application is externally accessible and if the attacker has a valid application session.

Type of User	Application Session	Description
External/DMZ unauthenticated user	No	Access external URL
External/DMZ authenticated user	Yes	Any responsibility
Internal unauthenticated user	No	Access internal URL
Internal authenticated user	Yes	Any responsibility

Oracle EBS CPU Risks and Threats

The risk of Oracle E-Business Suite security vulnerabilities depends if the application is externally accessible and if the attacker has a valid application session.

Type of User	Application Session	Description
External/DMZ unauthenticated user	No	Access external URL
External/DMZ authenticated user	Yes	Any responsibility
Internal unauthenticated user	No	Access internal URL
Internal authenticated user	Yes	Any responsibility

Sample CPU Risk Mapping (last CPU July 2015)

Type of User	Number of Security Bugs	Notes
External unauthenticated user	42 (1)	▪ **19 of 42 are high risk**
External authenticated user	14 (1)	▪ 10 of 14 are exploited with only a valid application session
Internal unauthenticated user	197	▪ **Many are high risk**
Internal authenticated user	35	▪ Most require access to specific module in order to exploit

(1) Assumes URL firewall is enabled and count is for all external “i” modules (iSupplier, iStore, etc.).

SQL Injection Explained

Attacker modifies URL with extra SQL

```
http://<server>/pls/VIS/fnd_gfm.dispatch?
p_path=fnd_help.get/US/fnd/@search');%20f
nd_user_pkg.updateUser('SYSADMIN',%20'SEE
D',%20'welcome1
```

Oracle EBS executes appends SQL to the SQL statement being executed

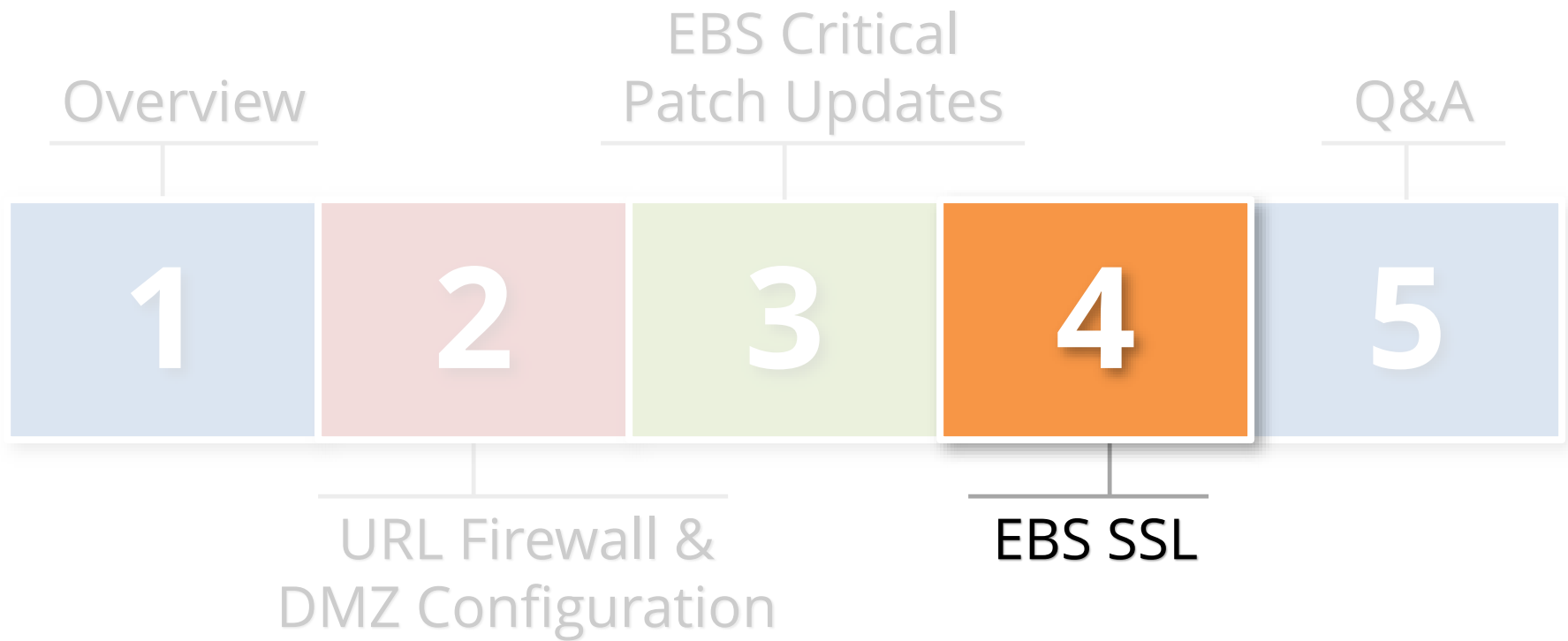
- SQL executed as APPS database account
- Example changes any application account password

This vulnerability was patched as part of Oracle Security Alert #32

Common Mistakes

Mistake	Impact	Risk
Oracle Critical Patch Update (CPU) EBS security patches not being routinely applied	▪ Many SQL injection and other high risk vulnerabilities are unpatched ▪ Number of vulnerabilities can be exploited even if DMZ is properly configured with URL Firewall and Node Trust Level ▪ Most EBS vulnerabilities not blocked by commercial Web Application Firewalls or other security tools ▪ Must use an EBS specific security tool to block known and 0-day security vulnerabilities, such as AppDefend	Critical

Agenda


Overview
EBS Critical Patch Updates
Q&A
1
2
3
4
5
URL Firewall & DMZ Configuration
EBS SSL

Oracle EBS SSL MOS Notes

Enabling SSL for Oracle E-Business Suite in a DMZ requires a complex setup because of certificates. Follow the steps for configuring SSL in the "Middle Tier." SSL configuration was updated in July 2016 to support TLS 1.1 and TLS 1.2.

"Enabling SSL/TLS in Oracle E-Business Suite"

12.2	1367293.1 (Previous 2143101.1)
12.1/12.0	2143099.1 (Previous 376700.1)
11i	123718.1

Oracle EBS HTTP Network Traffic

```
POST
http://oa.integrigy.com:8010/OA_HTML/OA.jsp?
page=/oracle/apps/fnd/sso/login/webui/MainLo
ginPG HTTP/1.1

_AM_TX_ID_FIELD=1wcuM2LWP
_FORM=DefaultFormNameKBTL4xsJ
usernameField=SYSADMIN
passwordField=MYPASSWORD
SubmitButton%24%24unvalidated=falseI_3t5ZET
```

Using SSL Encryption

Encrypt all end-user traffic externally as well as internally.

1. **Use SSL encryption and acceleration on load balancers**
   - Simplifies setup and configuration
   - Removes load from application servers to load balancer with dedicated SSL encryption hardware
2. **Implement SSL on Oracle EBS Application Servers**
   - Use Oracle's MOS SSL Notes
   - ***Be sure to disable SSLv2, SSLv3, and weak ciphers***

Common Mistakes

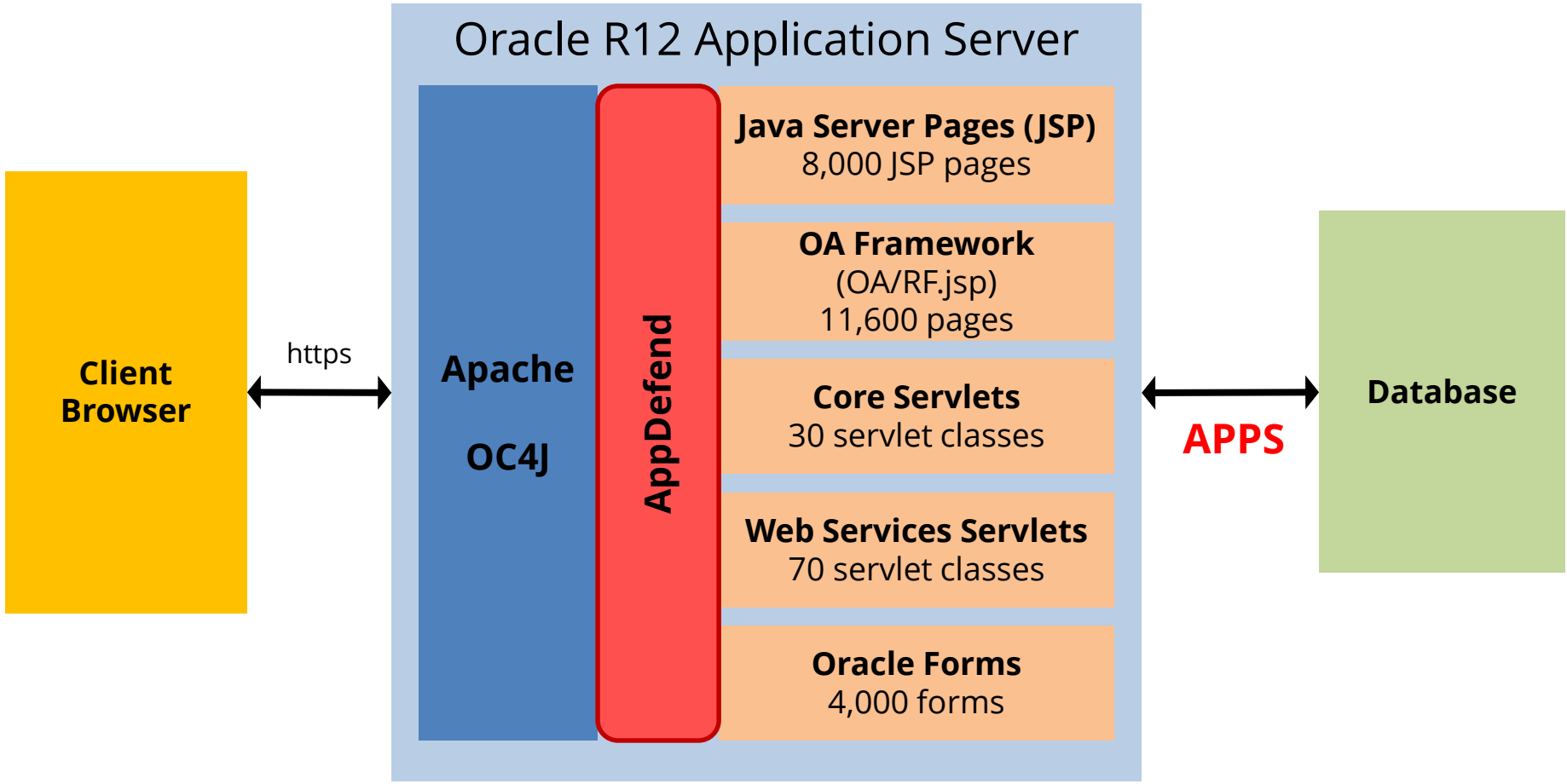
Mistake	Impact	Risk
Using Oracle EBS native SSL encryption rather than SSL termination on the reverse proxy or load balancer	▪ EBS SSL components slow to be updated and behind in support for newer protocols and ciphers ▪ Native EBS SSL maintained by DBAs rather than network administrators resulting	Medium
[If EBS native SSL is used] **SSL is not patched and updated to latest**	▪ Must update and patch to support latest versions of SSL/TLS (TLS 1.1 and TLS 1.2) updated in July 2016	Medium
[If EBS native SSL is used] **Protocols and cipher suites are not**	▪ Must disable SSLv2, SSLv3, and weak ciphers	Medium

Integrigy AppDefend

AppDefend is an **enterprise application firewall** designed and optimized for the Oracle E-Business Suite.

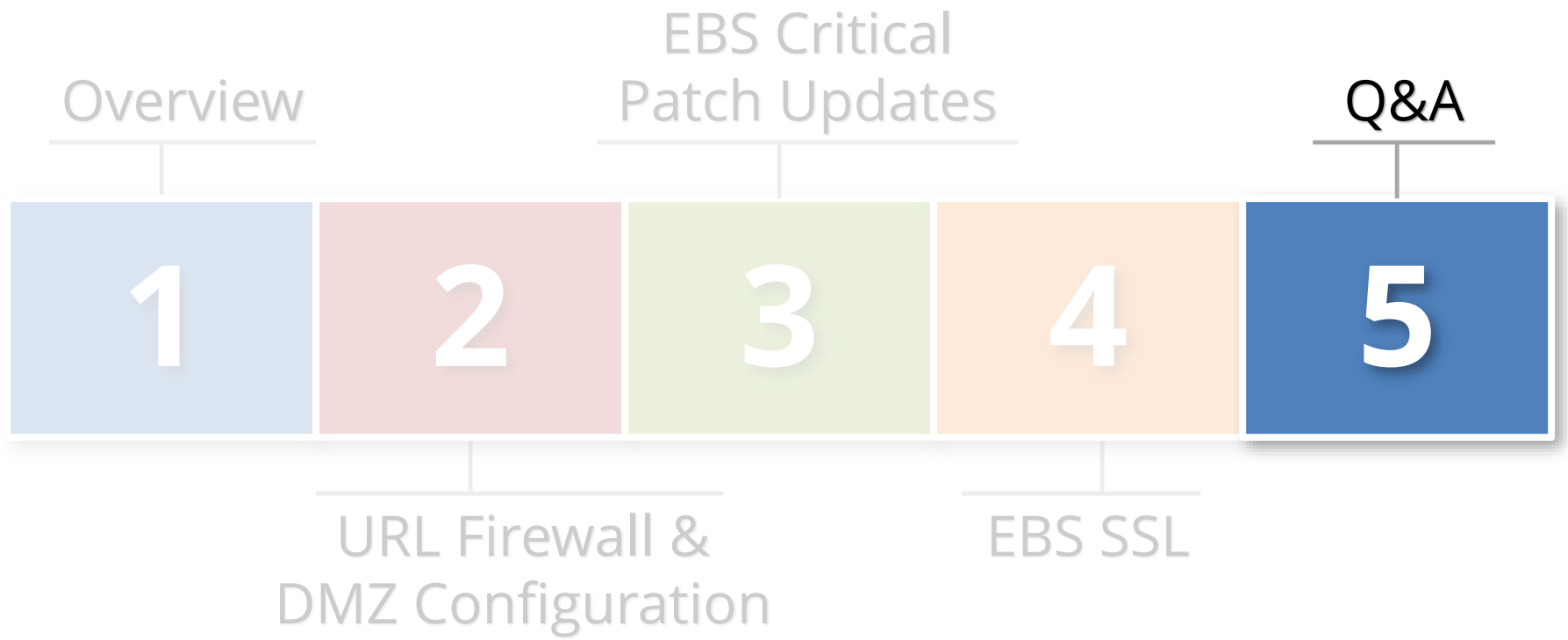
- **Prevents Web Attacks**
  Detects and reacts to SQL Injection, XSS, and known Oracle EBS vulnerabilities
- **Limits EBS Modules**
  More flexibility and capabilities than URL firewall to identify EBS modules
- **Application Logging**
  Enhanced application logging for compliance requirements like PCI-DSS 10.2
- **Protects Web Services & Mobile**
  Detects and reacts to attacks against native Oracle EBS web services (SOA, SOAP, REST) and Oracle EBS Mobile applications

AppDefend and Oracle EBS 12.0 & 12.1



- **AppDefend** runs within the Oracle E-Business OC4J containers as a servlet filter and monitors all incoming requests and out-going responses. Being in the OC4J container, AppDefend can access all session state, attributes, error messages, and the database.

Agenda


Overview
EBS Critical Patch Updates
Q&A
1
2
3
4
5
URL Firewall & DMZ Configuration
EBS SSL

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**