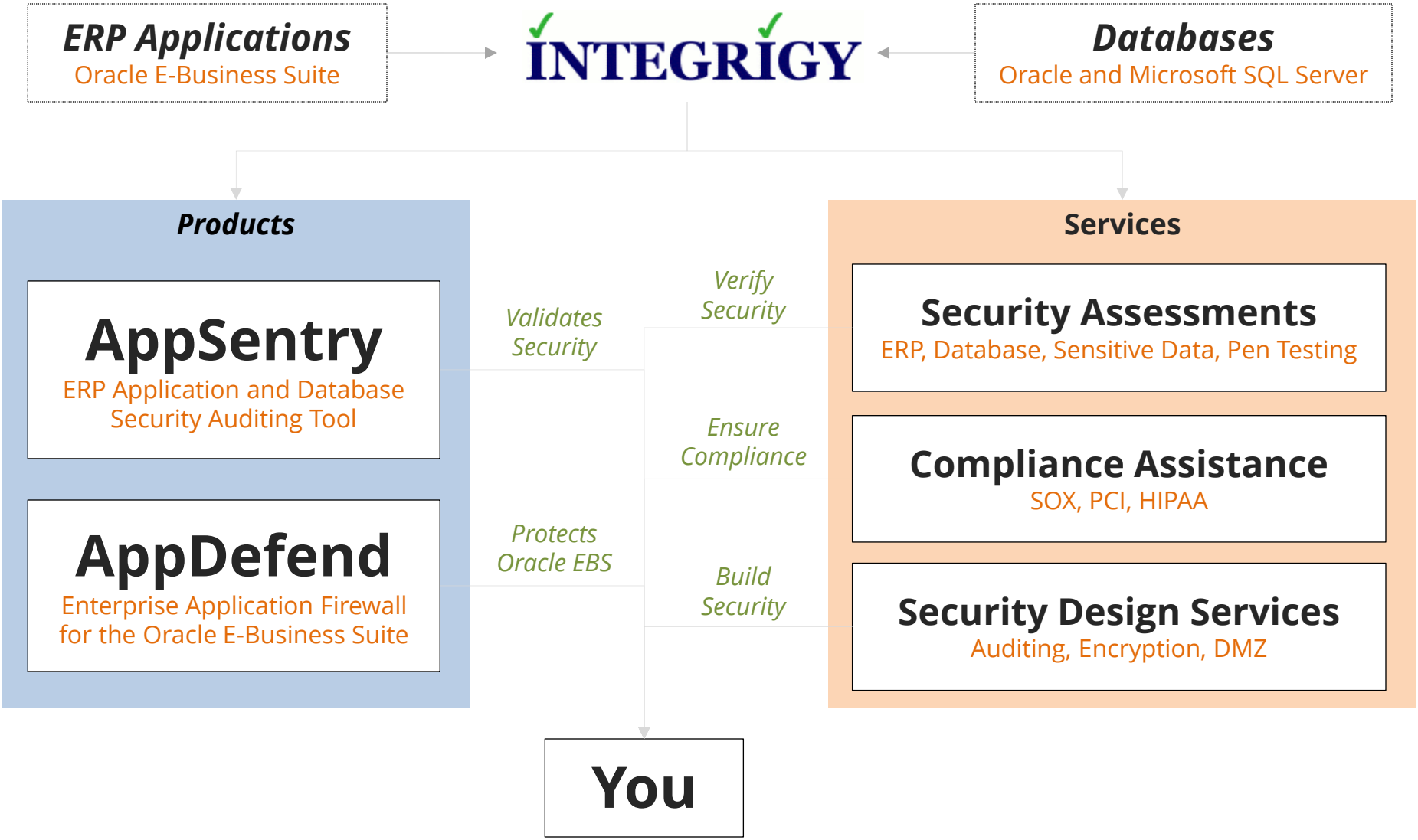
When You Can't Apply Oracle Security Patches

June 25, 2013

Stephen Kost
Chief Technology Officer
Integrigy Corporation

About Integrigy



Oracle Database

Why are CPU Patches Not Applied?

Oracle Database Critical Patch Updates (CPU) are not applied to many production databases due to testing, support, downtime, and application issues.

- **Lack of IT Management and DBA prioritization of security patches and periodic database upgrades**
  - Significant effort to apply and test security patches
  - Security patches may require a database upgrade
- **Limitations on applying database security patches**
  - Application may not support a database upgrade
  - No downtime window available

Quiz – Database CPU

ACTION_TIME	ACTION	VERSION	COMMENTS
18-JUN-08 03.13.45.093449 PM	UPGRADE	10.2.0.3.0	Upgraded from 9.2.0.8.0
18-JAN-09 06.51.32.425375 AM	APPLY	10.2.0.4	CPUJan2009
09-APR-09 04.48.14.903718 PM	UPGRADE	10.2.0.4.0	Upgraded from 10.2.0.3.0
18-AUG-09 08.50.30.021401 AM	APPLY	10.2.0.4	CPUJul2009
16-OCT-11 07.18.57.042620 AM	APPLY	10.2.0.4	CPUJul2011
27-FEB-13 06.42.55.108783 AM	UPGRADE	11.2.0.2.0	Upgraded from 10.2.0.4.0

What CPU Level is this database patched to?

A. July 2009 **B. January 2011** **C. July 2011** **D. January 2013**

Quiz – Database CPU

ACTION_TIME	ACTION	VERSION	COMMENTS
18-JUN-08 03.13.45.093449 PM	UPGRADE	10.2.0.3.0	Upgraded from 9.2.0.8.0
18-JAN-09 06.51.32.425375 AM	APPLY	10.2.0.4	CPUJan2009
09-APR-09 04.48.14.903718 PM	UPGRADE	10.2.0.4.0	Upgraded from 10.2.0.3.0
18-AUG-09 08.50.30.021401 AM	APPLY	10.2.0.4	CPUJul2009
16-OCT-11 07.18.57.042620 AM	APPLY	10.2.0.4	CPUJul2011
27-FEB-13 06.42.55.108783 AM	UPGRADE	11.2.0.2.0	Upgraded from 10.2.0.4.0

What CPU Level is this database patched to?

A. July 2009 **B. January 2011** **C. July 2011** **D. January 2013**

Critical Patch Updates Database Baselines

Database Version Upgrade Patch	Included CPU
10.2.0.4	April 2008
10.2.0.5	October 2010
11.1.0.6	October 2007
11.1.0.7	January 2009
11.2.0.1	January 2010
11.2.0.2	January 2011
11.2.0.3	July 2011

At time of release, the latest <u>available</u> CPU is included.

CPU Baselines and Terminal Patches

Database Version Upgrade Patch	Included CPU	Terminal CPU
10.2.0.4	April 2008	**July 2011**
10.2.0.5	October 2010	July 2013 (ES)
11.1.0.6	October 2007	**July 2009**
11.1.0.7	January 2009	July 2015
11.2.0.1	January 2010	**July 2011**
11.2.0.2	January 2011	October 2013
11.2.0.3	July 2011	TBD

ES = Extended Support TBD = Date not yet announced

Oracle 11.2.0.2 Scenario

Oracle 11.2.0.2 database installed with no CPU applied, so missing April 2011 through April 2013. Client unable to apply CPUs due to limited IT resources and outsourcer.

- **Application vendor has not yet certified 11.2.0.3 for use with primary database application.**
  - CPU support will end with October 2013 CPU
- **CPU was not applied when database was upgraded.**
  - Database CPU level reset to January 2011 during upgrade in February 2013 – January 2012 CPU had been applied previously
- **No CPUs applied due to limited IT resources**
  - Missing 9 CPUs – 29 unpatched security vulnerabilities

Oracle Database CPU Risks and Threats

The risk of Oracle database security vulnerabilities depends if an attacker has a database account or can obtain a database account.

Type of User	Database Account	Description
Unauthenticated user	No	Can connect to database listener if IP address, port, SID is known
Low privileged user	Yes	Only PUBLIC privileges
Moderate privileged user	Yes	Some privileges
High privileged user	Yes	DBA like privileges

11.2.0.2 CPU Risk Mapping

Type of User	Number of Security Bugs	Notes
Unauthenticated user No database account	9	**1 – O5LOGON Authentication** 7 – Denial of service
Low privileged user Create session system privilege only	7	▪ **Averages one per CPU** ▪ **Requires only PUBLIC privileges**
Moderate privileged user Create table, procedure, index, etc.	6	▪ Usually requires CREATE PROCEDURE system privilege
High privileged user DBA, SYSDBA, local OS access, etc.	7	2 – SYSDBA privileges 3 – Advanced privileges 2 – Local OS access

#1 – Don’t Start Behind

<u>ALWAYS</u> install latest CPU with database installation or upgrades

- Database Install + **latest** CPU
- Database Upgrade + **latest** CPU

PSU = For production, use PSU from last test DB

SPU = For production, use latest SPU – low risk

Oracle Database Patch Set Update

- **April 2013 for 11.2.0.2 – Bug Fixes**
  - SPU = 29 only security fixes
  - **PSU = 409 security fixes + priority fixes**

- **PSU is a patching path**
  - Once applied, must always apply PSUs rather than CPUs until next database upgrade
  - CPUs apply to base version only – no PSU

Solutions by Risk for No CPUs

Type of User	Solutions if CPUs not applied
Unauthenticated user No database account	**#2 – Limit direct access to the database**
Low privileged user Create session system privilege only	#3 – Use only named accounts #4 – No generic read-only accounts
Moderate privileged user Create table, procedure, index, etc.	#5 – Limit privileges in production
High privileged user DBA, SYSDBA, local OS access, etc.	#6 – Use database vault #7 – External database auditing solution #8 – Limit OS access for prod to DBAs

#2 – Limit Database Access

1. **Enterprise firewall and VPN solutions**
   - Block all direct database access outside of the data center
2. **SQL*Net Valid Node Checking**
   - Included with database
   - Block access by IP address
3. **Oracle Connection Manager**
   - SQL*Net proxy server, included with database
   - Block access by IP address or range
4. **Oracle Database Vault**
   - Add-on database security product

Oracle E-Business Suite

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 unauthenticated user	No	Access external URL
External authenticated user	Yes	Any responsibility
Internal unauthenticated user	No	Access internal URL
Internal authenticated user	Yes	Any responsibility

Critical Patch Updates EBS Baselines

EBS Version	Included CPU
12.0.6	October 2008
12.1.1	April 2009
12.1.2	October 2009
12.1.3	July 2010

At time of release, the latest <u>available</u> CPU is included.

Critical Patch Update EBS Upgrade Impact

Type of Upgrade	Impact	Description
11.5 to 11.5 (11.5.9 → 11.5.10.2) **12.0 to 12.0 (12.0.4 → 12.0.6)** **12.1 to 12.1 (12.1.1 → 12.1.3)**	Low	▪ All files are versioned ▪ A few fixes may be reversed
11i to 12.x (11.5.10.2 → 12.1.3)	High	▪ 11i and R12 version numbers are different ▪ ALL fixes will be reversed
12.0 to 12.1 (12.0.6 → 12.1.3)	Moderate	▪ 12.0 and 12.1 version numbers can be different ▪ Most fixes will be reversed

#1 – Don’t Start Behind

<u>ALWAYS</u> install latest CPU with application installation or upgrades

- EBS Install + **latest** CPU
- EBS Upgrade + **latest** CPU

12.1.3 CPU Risk Mapping

Type of User	Number of Security Bugs	Notes
External unauthenticated user	18 (1)	▪ **16 of 18 are high risk**
External authenticated user	5 (1)	▪ 3 of 5 are exploited with only a valid application session
Internal unauthenticated user	34	▪ **Most are high risk**
Internal authenticated user	12	▪ 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.).

Solutions by Risk for No CPUs

Type of User	Solutions if CPUs not applied
External unauthenticated user	**#2 – Enable Oracle EBS URL firewall** **#3 – Implement Integrigy's AppDefend**
External authenticated user	#4 – Enable Oracle EBS external responsibilities
Internal unauthenticated user	#5 – Implement Integrigy's AppDefend
Internal authenticated user	#6 – Limit access to privileged responsibilities

Oracle EBS DMZ MOS Notes

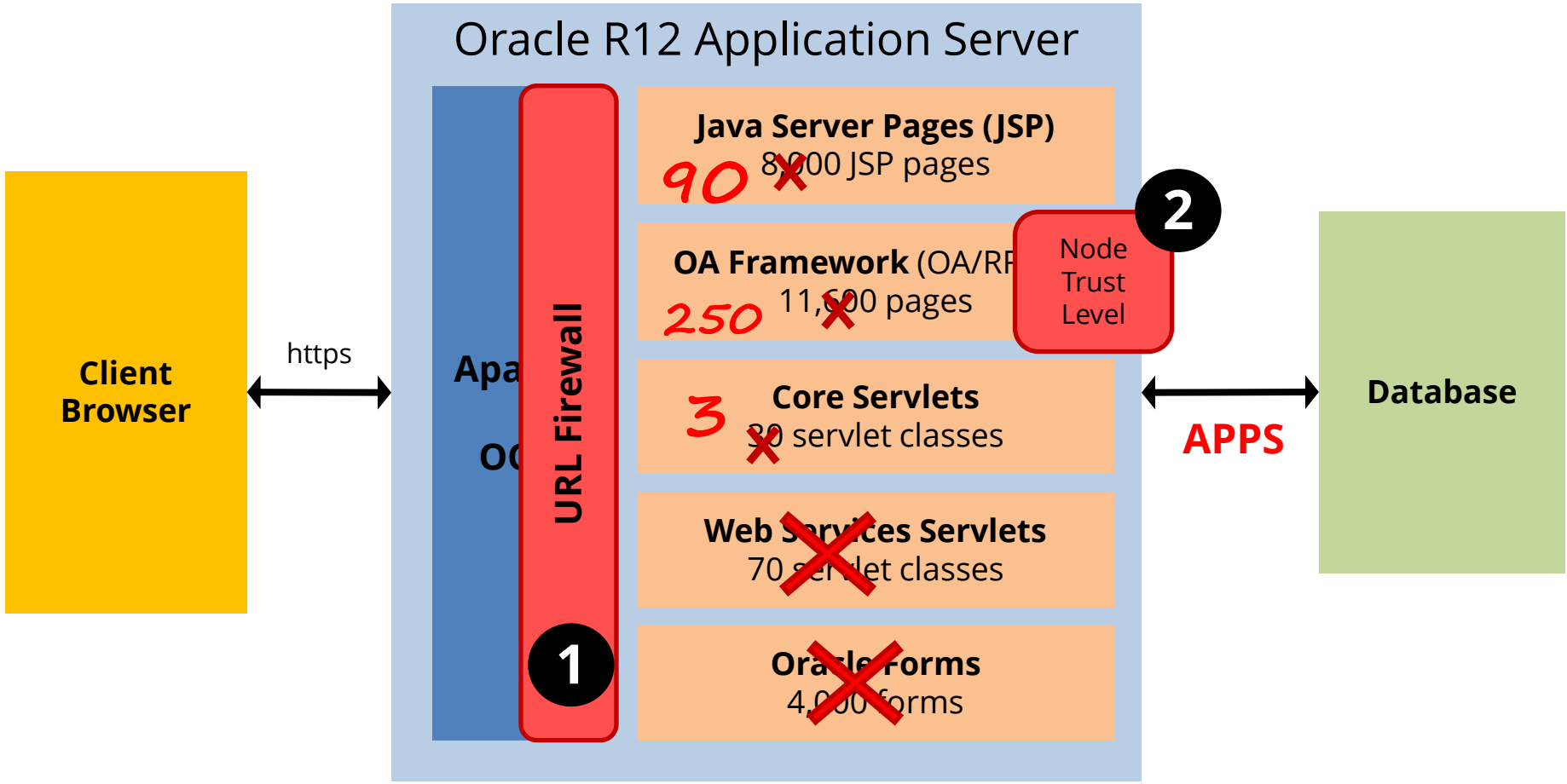
Deploying Oracle E-Business Suite in a DMZ requires a specific and detailed configuration of the application and application server. All steps in the Oracle provided MOS Note must be followed.

380490.1 *Oracle E-Business Suite* ***R12*** *Configuration in a DMZ*

287176.1 *DMZ Configuration with Oracle E-Business Suite* ***11i***

MOS = My Oracle Support

Oracle EBS 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.

Integrigy AppDefend for R12

AppDefend is an **enterprise application firewall** designed and optimized for the Oracle E-Business Suite R12.

- **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**
  Detects and reacts to attacks against native Oracle EBS web services (SOA, SOAP, REST)

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**