INTEGRIGY

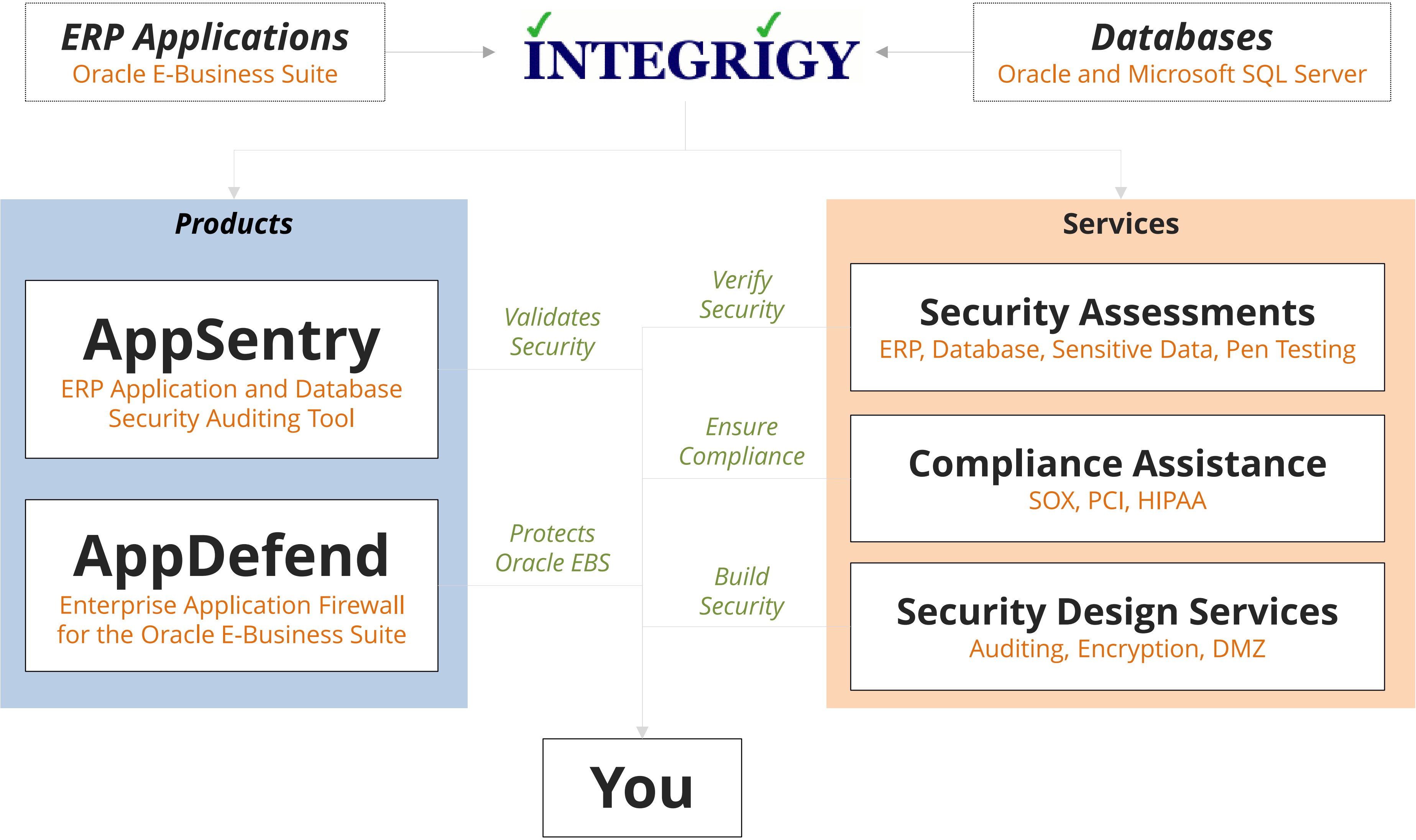
Going Without CPU Patches on Oracle E-Business Suite 11i?

September 17, 2013

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

About Integrigy



ERP Applications
Oracle E-Business Suite

INTEGRIGY

Databases
Oracle and Microsoft SQL Server

Products

AppSentry
ERP Application and Database Security Auditing Tool

AppDefend
Enterprise Application Firewall for the Oracle E-Business Suite

Validates Security

Protects Oracle EBS

Services

Security Assessments
ERP, Database, Sensitive Data, Pen Testing

Compliance Assistance
SOX, PCI, HIPAA

Security Design Services
Auditing, Encryption, DMZ

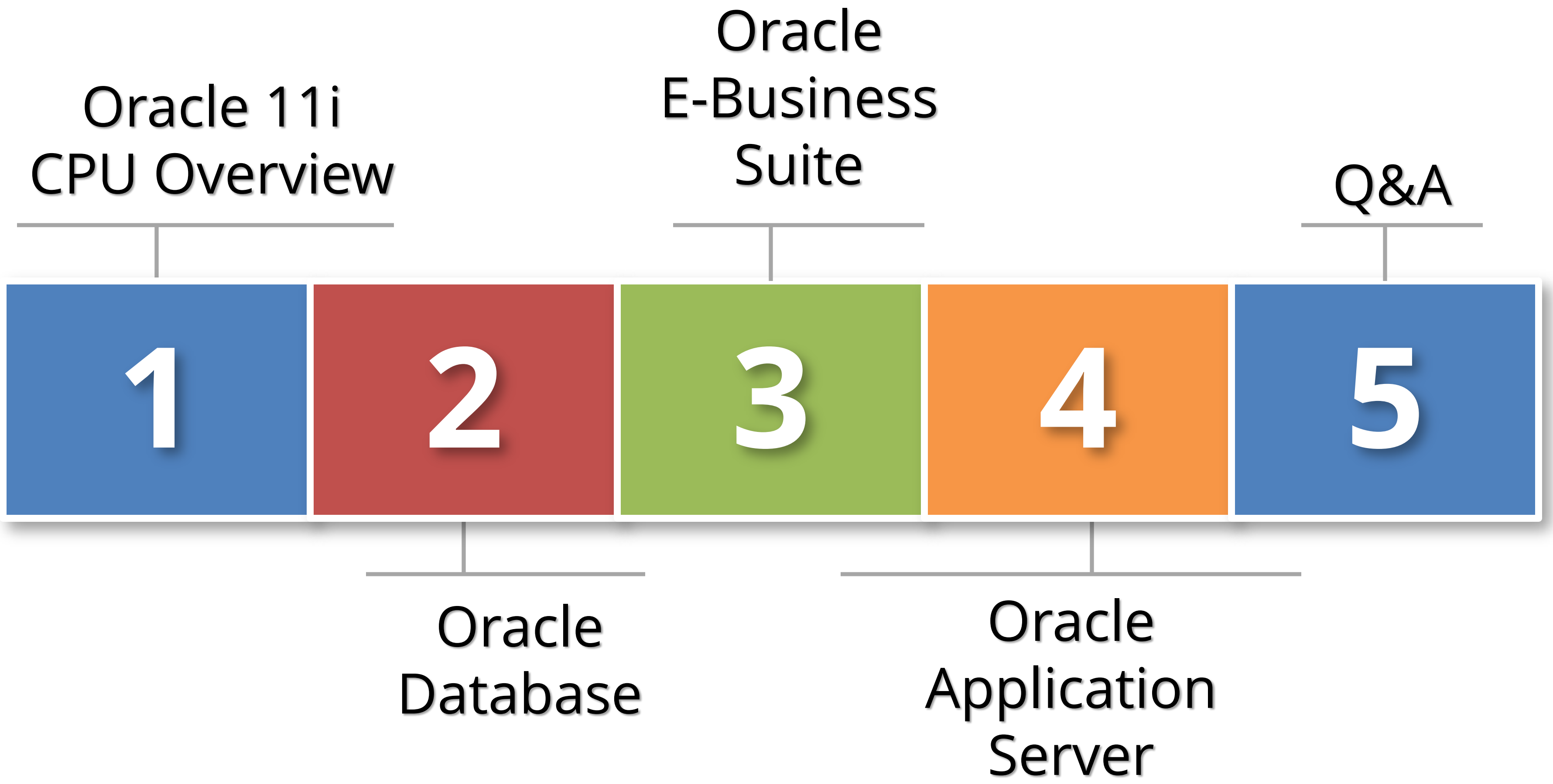
Verify Security

Ensure Compliance

Build Security

You

Agenda



1 Oracle 11i CPU Overview

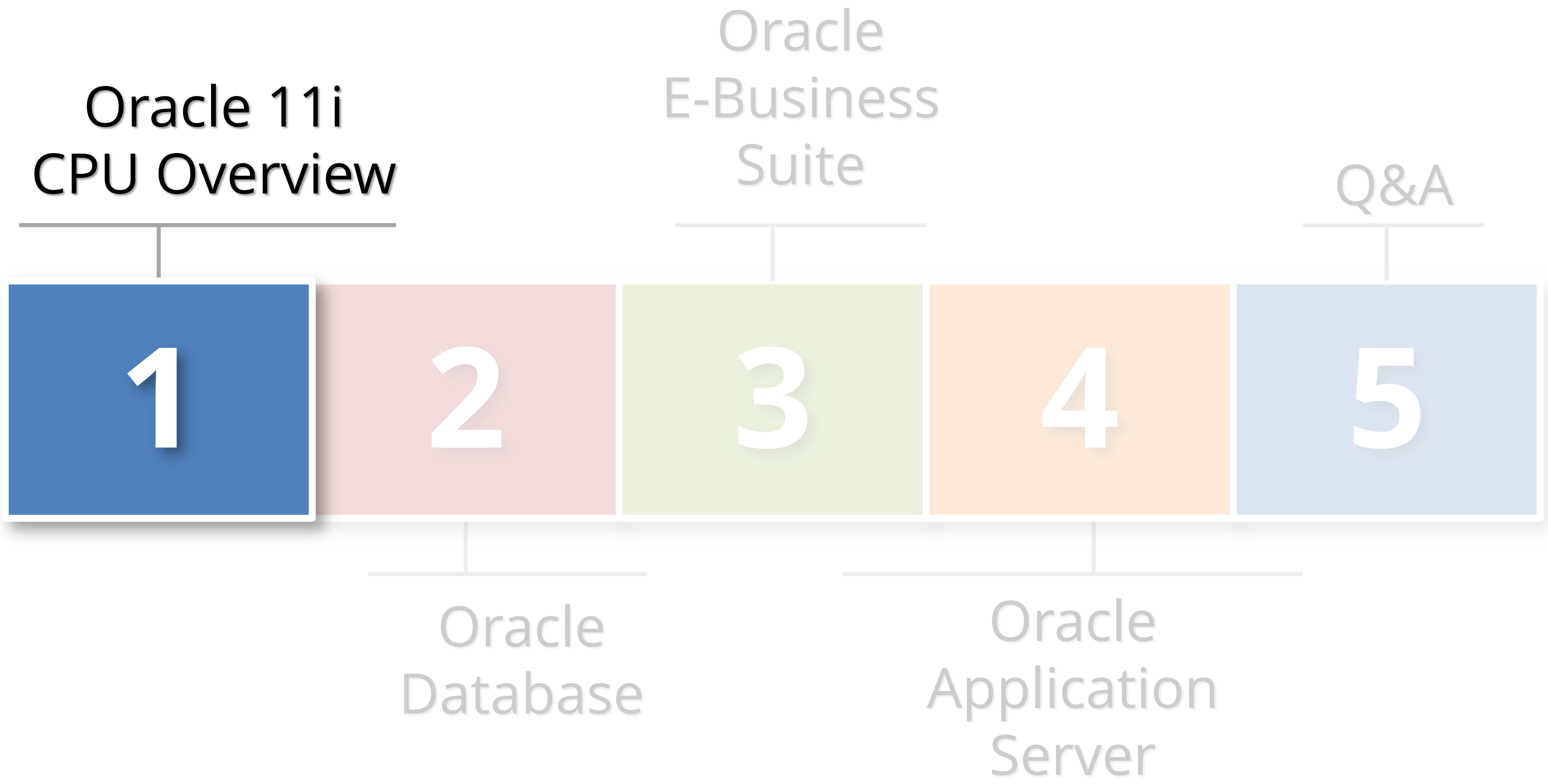
2 Oracle Database

3 Oracle E-Business Suite

4 Oracle Application Server

5 Q&A

Agenda



1 Oracle 11i CPU Overview

2 Oracle Database

3 Oracle E-Business Suite

4 Oracle Application Server

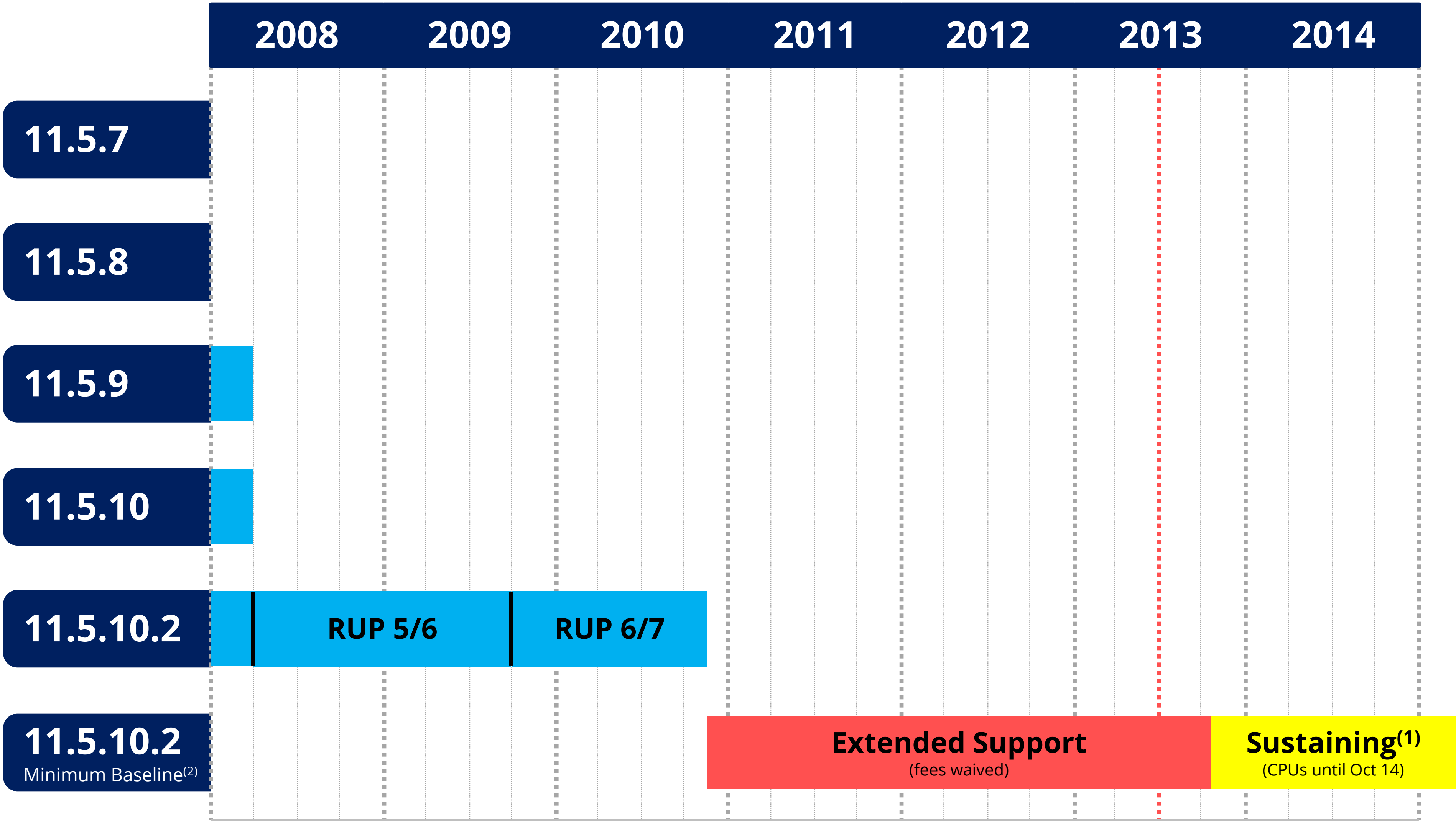
5 Q&A

Why are CPU Patches Not Applied?

Oracle Critical Patch Updates (CPU) are not applied to many 11i environments due to support, testing, downtime, and application issues.

- **Lack of IT Management and DBA prioritization of security patches and periodic technical upgrades**
- **Unsupported application or database versions**
  - Must be on the 11i minimum baseline
- **Dropped Oracle Support or using third-party support**
  - Oracle CPU patches require current Oracle Support

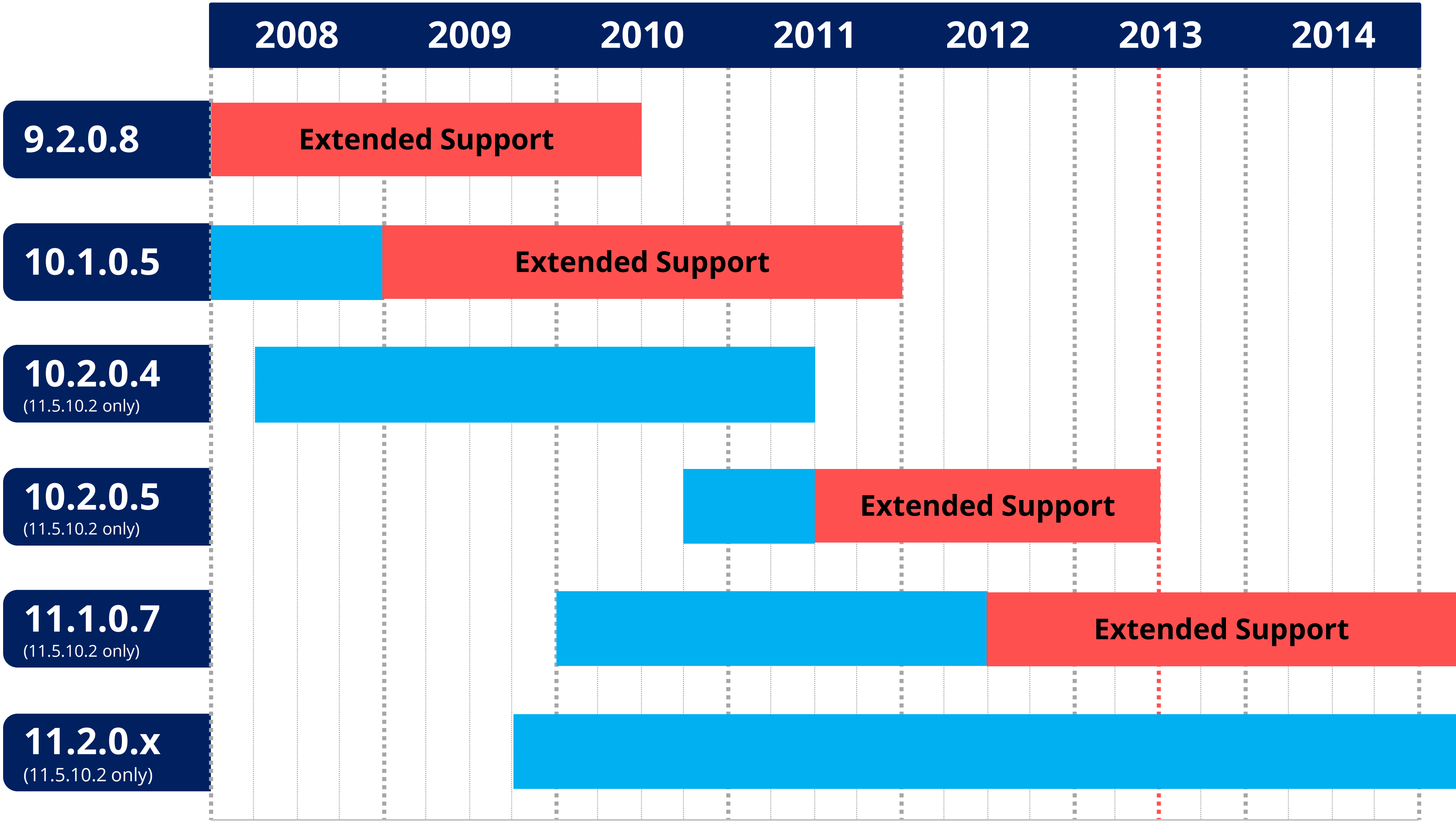
Oracle E-Business Suite CPU Support



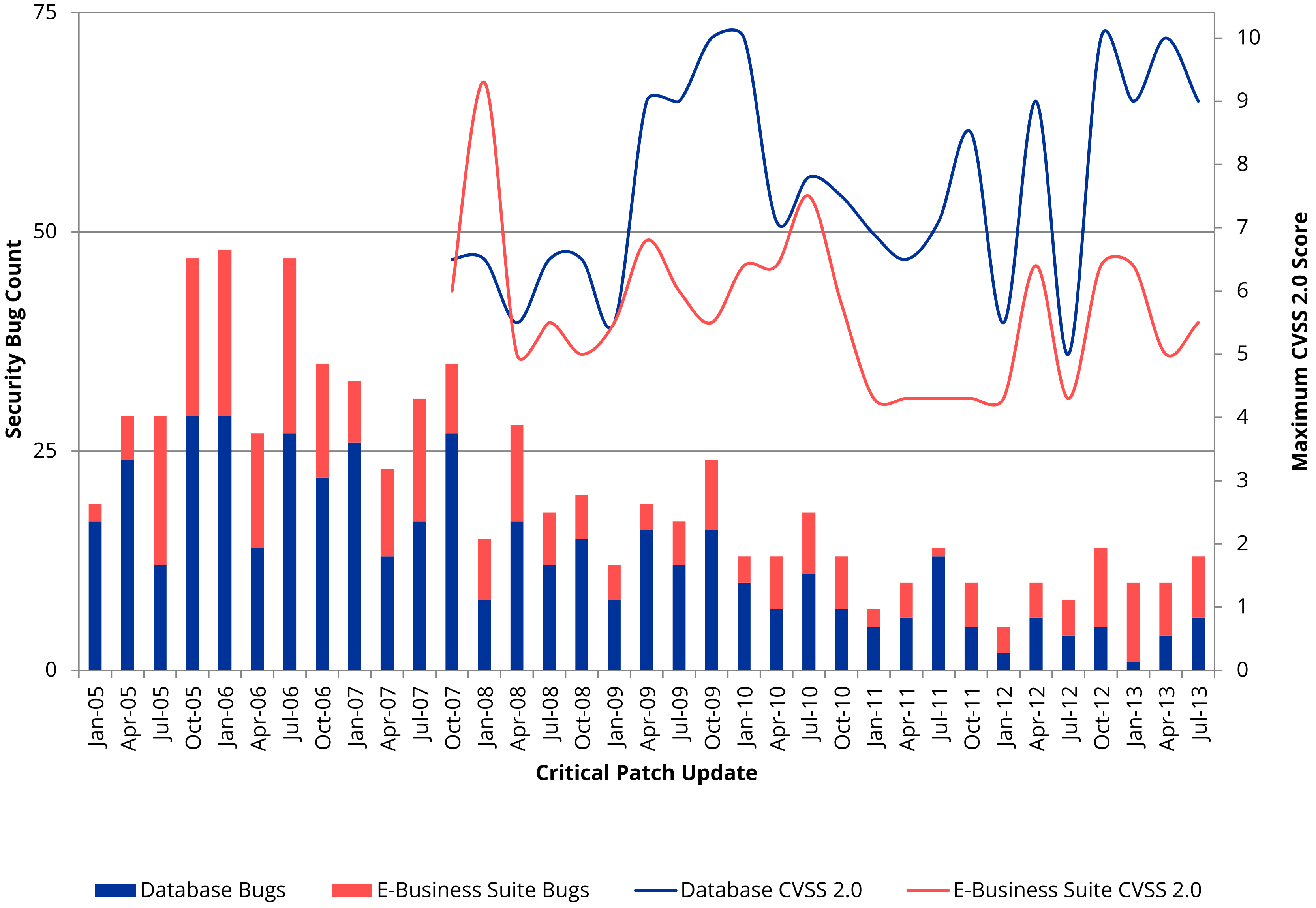
(1) See My Oracle Support Doc ID 1495337.1 - **11i last CPU is October 2014**

(2) See My Oracle Support Doc ID 883202.1

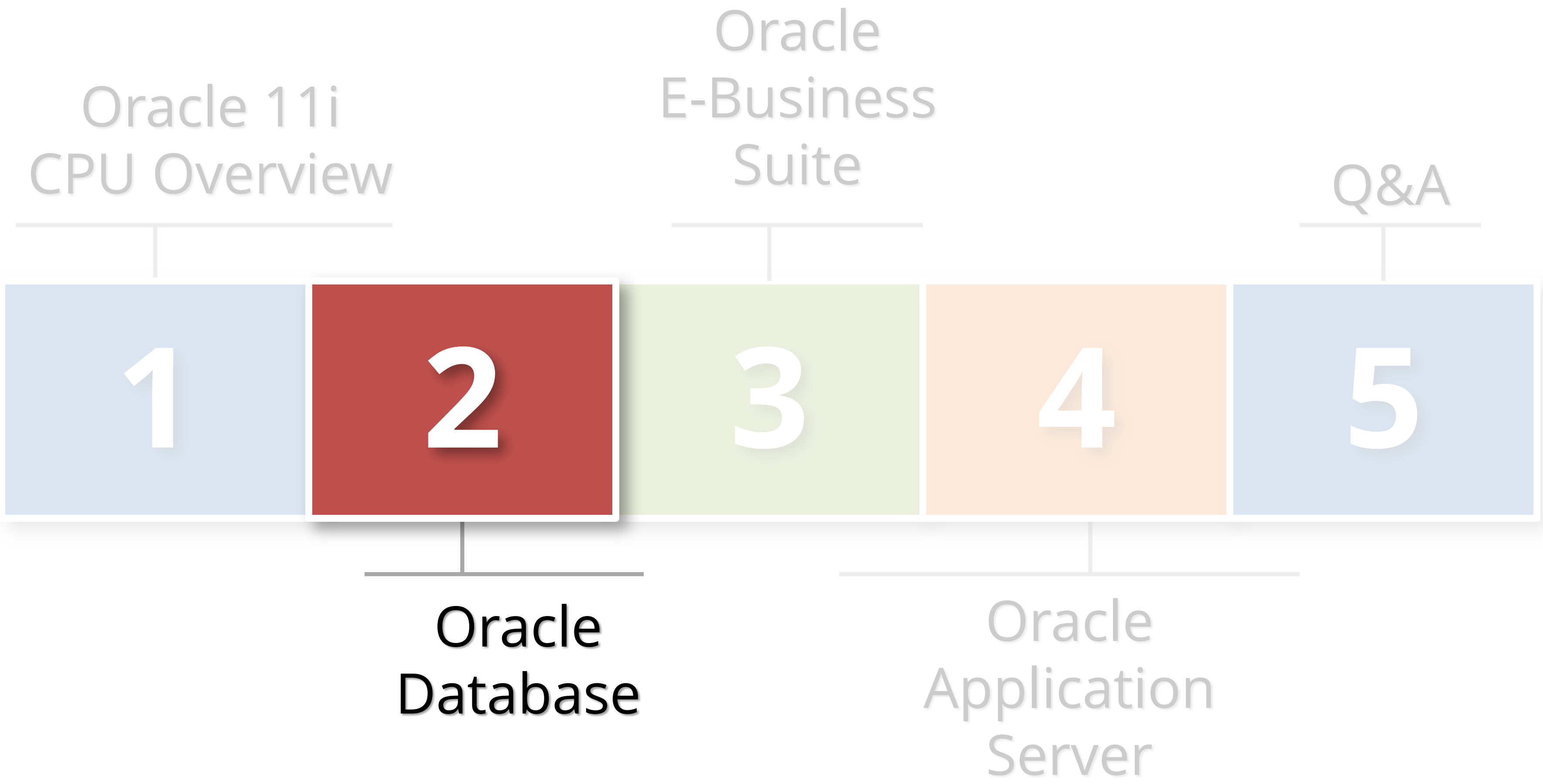
Oracle Database CPU Support



Security Vulnerabilities per Quarter



Agenda



1 Oracle 11i CPU Overview

2 Oracle Database

3 Oracle E-Business Suite

4 Oracle Application Server

5 Q&A

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 available 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

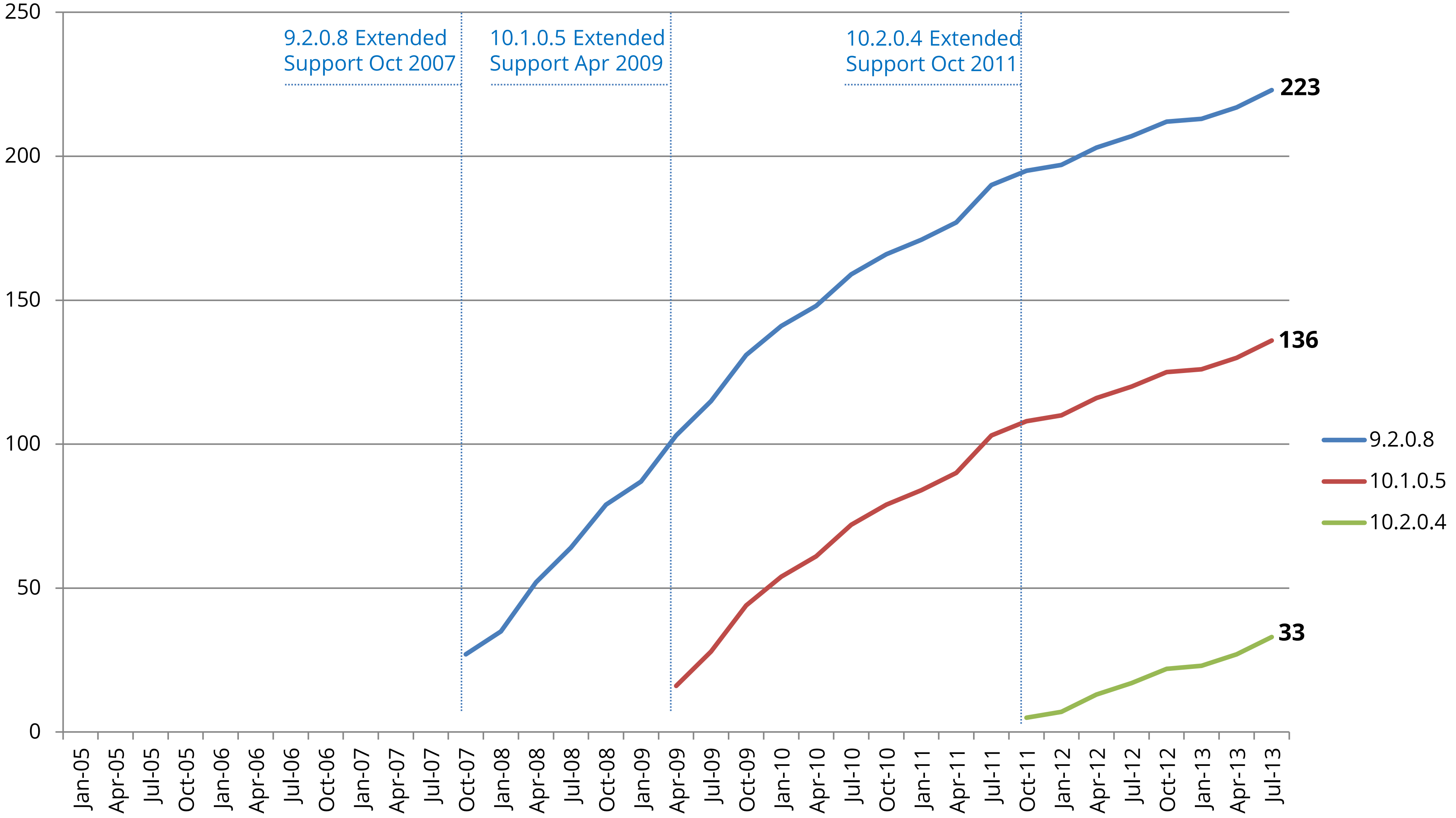
ES = Extended Support   TBD = Date not yet announced

Oracle 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

Cumulative Vulnerabilities per DB Version



Cumulative maximum count of open security vulnerabilities assuming no Critical Patches have been applied since the start of Extended Support

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 (DoS)
Low privileged user Create session system privilege only	7	▪ **Averages one per CPU** ▪ **Requires only PUBLIC privileges (APPLSYSPUB!!!)**
Moderate privileged user Create table, procedure, index, etc.	6	▪ Usually requires CREATE PROCEDURE system privilege
High privileged user DBA's, local OS access, etc.	7	2 – SYSDBA privileges 3 – Advanced privileges 2 – Local OS access

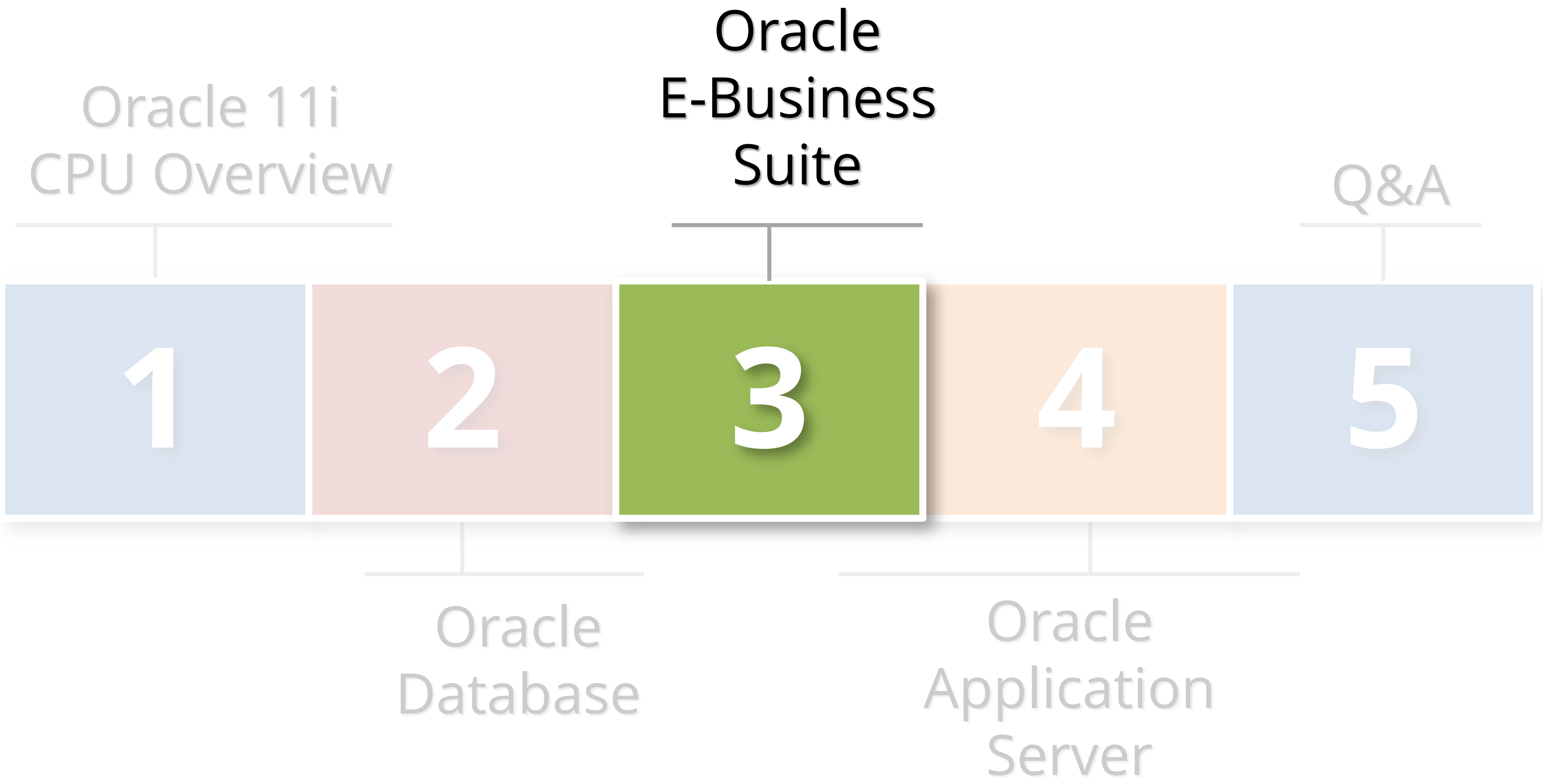
Solutions by Risk for No CPUs

Type of User	Solutions if CPUs not applied
Unauthenticated user No database account	**#1 – Limit direct access to the database** #2 – Use only named accounts #3 – No generic read-only accounts #4 – Change APPLSYSPUB password #5 – Check for default passwords
Low privileged user Create session system privilege only	
Moderate privileged user Create table, procedure, index, etc.	#6 – Limit privileges in production
High privileged user DBA, SYSDBA, local OS access, etc.	#7 – Use Oracle Database Vault #8 – External database auditing solution #9 – Limit OS access for prod to DBAs

#1 – Limit Database Access

1. **Enterprise firewall and VPN solutions**
   - At least 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

Agenda



1 Oracle 11i CPU Overview

2 Oracle Database

3 Oracle E-Business Suite

4 Oracle Application Server

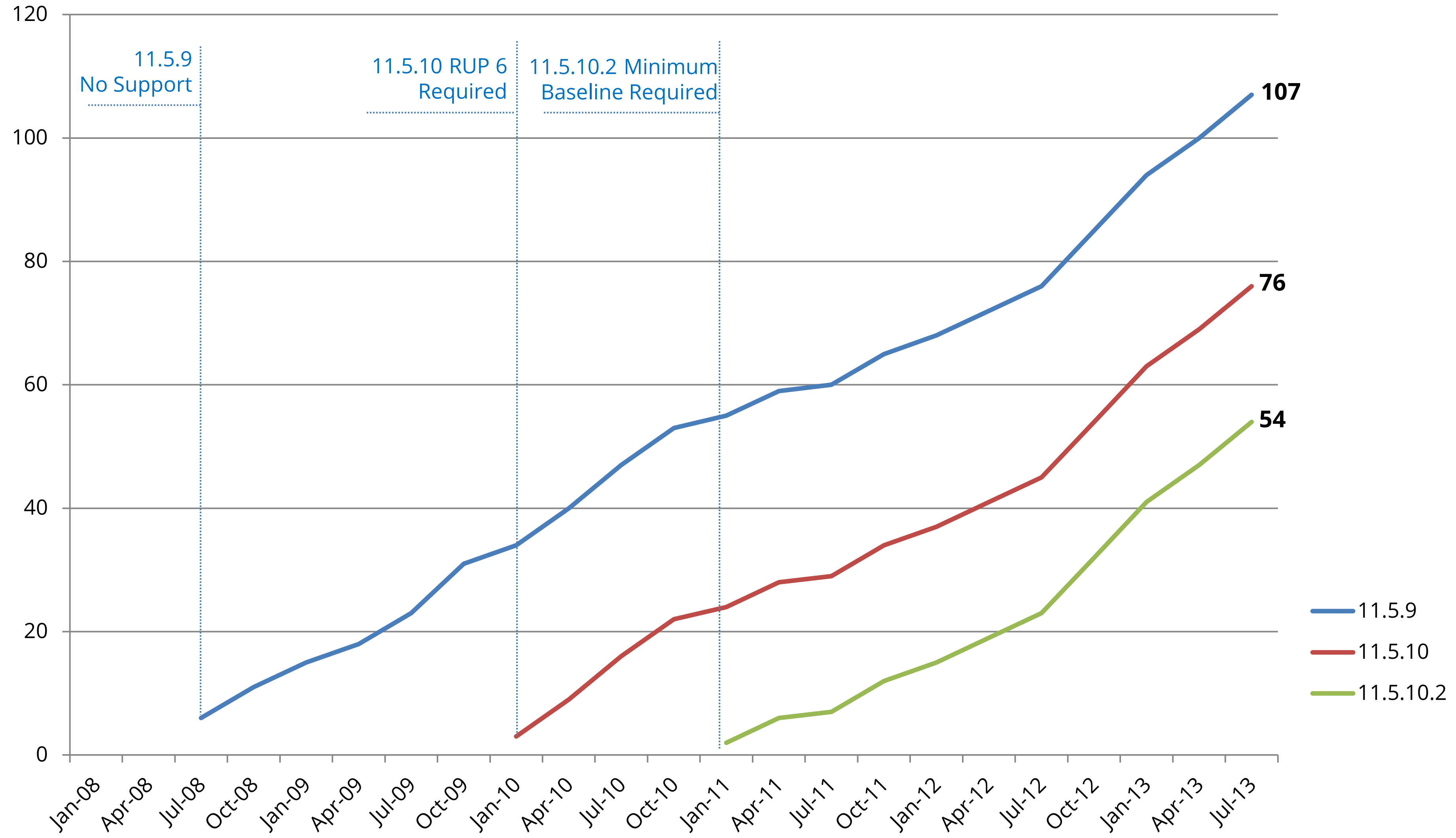
5 Q&A

Critical Patch Updates EBS 11i Baselines

EBS Version	Included CPU
11.5.9	CPUs were not available yet
11.5.10	April 2005
11.5.10.2	July 2005
12.0.6	October 2008
12.1.3	July 2010

At time of release, the latest available CPU is included.

Cumulative Vulnerabilities per 11i Version



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

11.5.10.2 CPU Risk Mapping

Type of User	Number of Security Bugs	Notes
External unauthenticated user	21 [1]	- **17 of 21 are high risk**
External authenticated user	6 [1]	- 3 of 6 are exploited with only a valid application session
Internal unauthenticated user	17	- **Many are high risk**
Internal authenticated user	10	- 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	#1 – Enable Oracle EBS URL firewall #2 – Implement Integrigy’s AppDefend
External authenticated user	#3 – Enable Oracle EBS external responsibilities
Internal unauthenticated user	#4 – Implement Integrigy’s AppDefend
Internal authenticated user	#5 – Limit access to privileged responsibilities

Oracle EBS DMZ MOS Notes

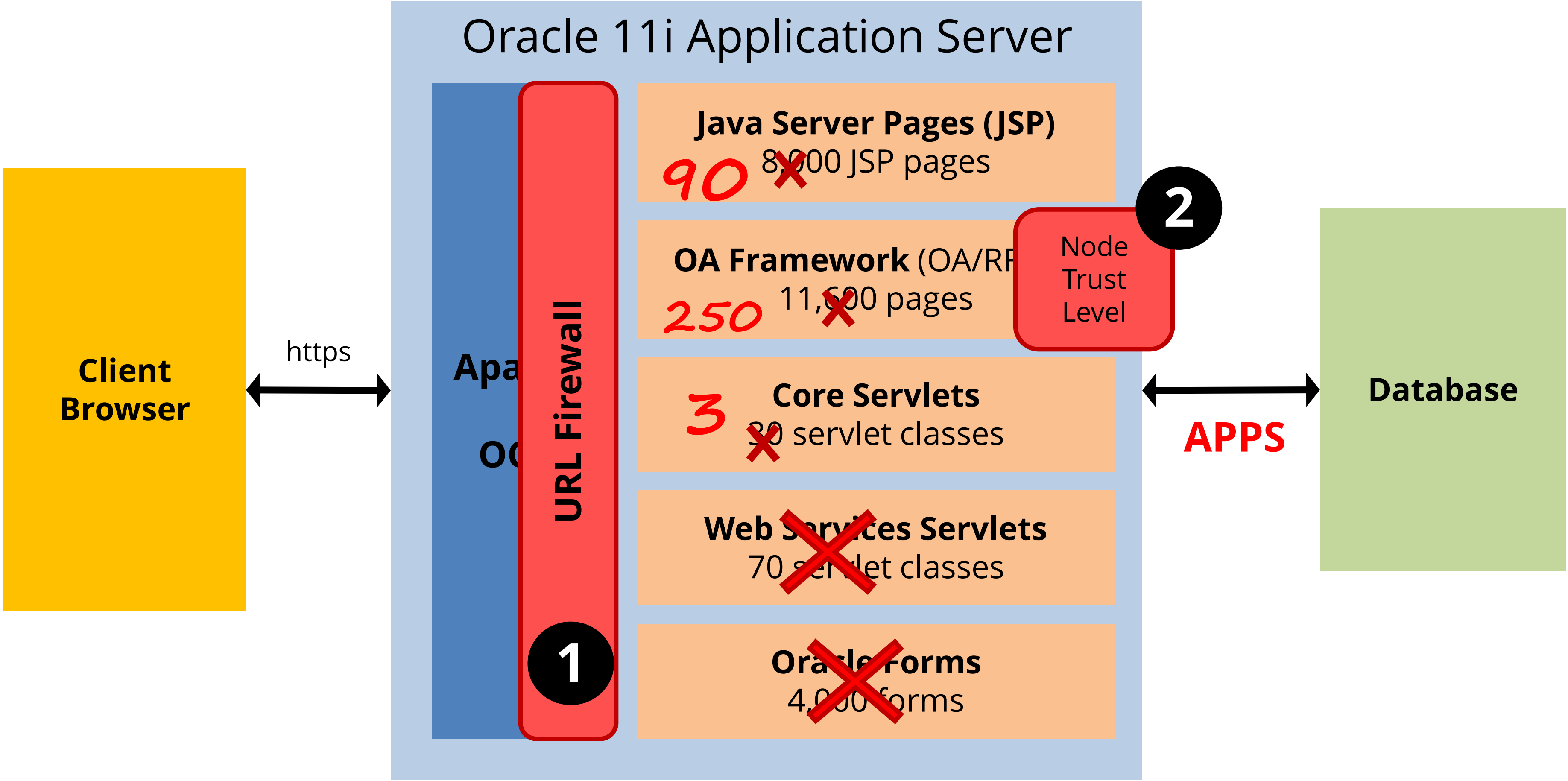
Deploying Oracle E-Business Suite in a DMZ requires a specific and detailed configuration of the application and application server. All steps in the Oracle provided MOS Note must be followed.

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

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

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 Oracle EBS

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

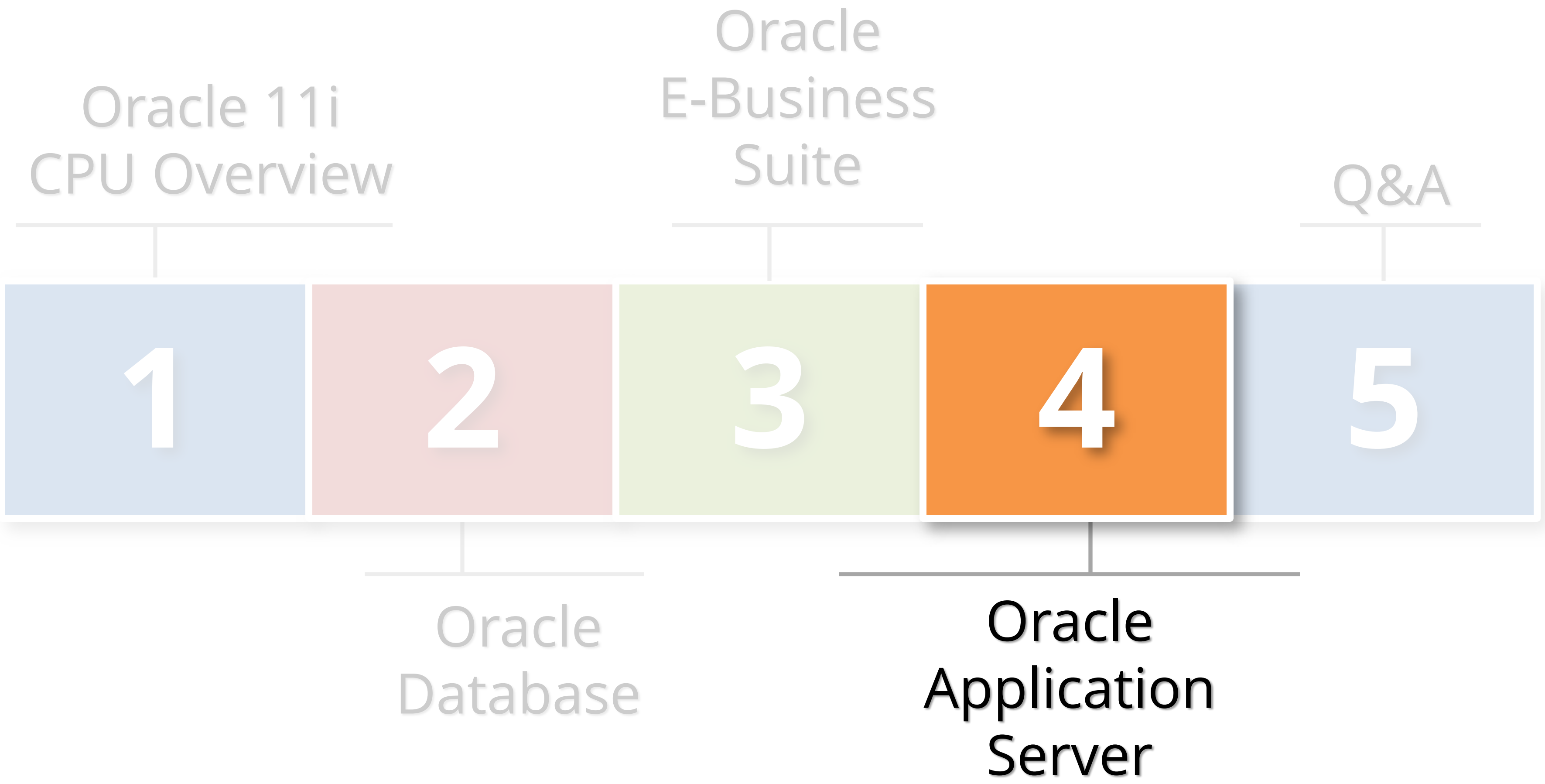
- **Prevents Web Attacks**
  Detects and reacts to SQL Injection, XSS, and known Oracle EBS vulnerabilities

- **Application Logging**
  Enhanced application logging for compliance requirements like PCI-DSS 10.2

- **Limits EBS Modules**
  More flexibility and capabilities than URL firewall to identify EBS modules

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

Agenda



1 Oracle 11i CPU Overview

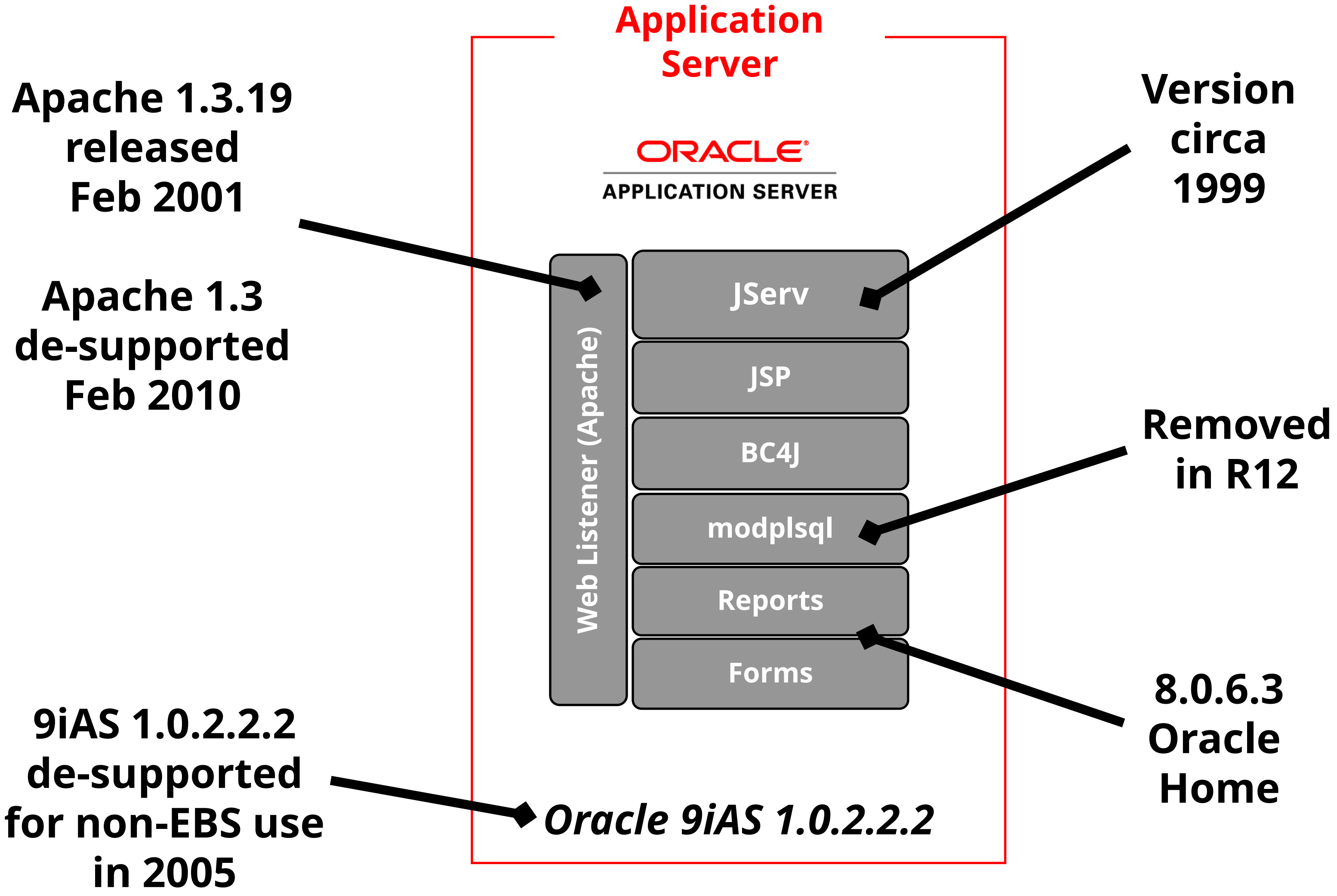
2 Oracle Database

3 Oracle E-Business Suite

4 Oracle Application Server

5 Q&A

11.5.10.2 Application Server



Apache 1.3.19 released Feb 2001

Apache 1.3 de-supported Feb 2010

9iAS 1.0.2.2.2 de-supported for non-EBS use in 2005

Version circa 1999

Removed in R12

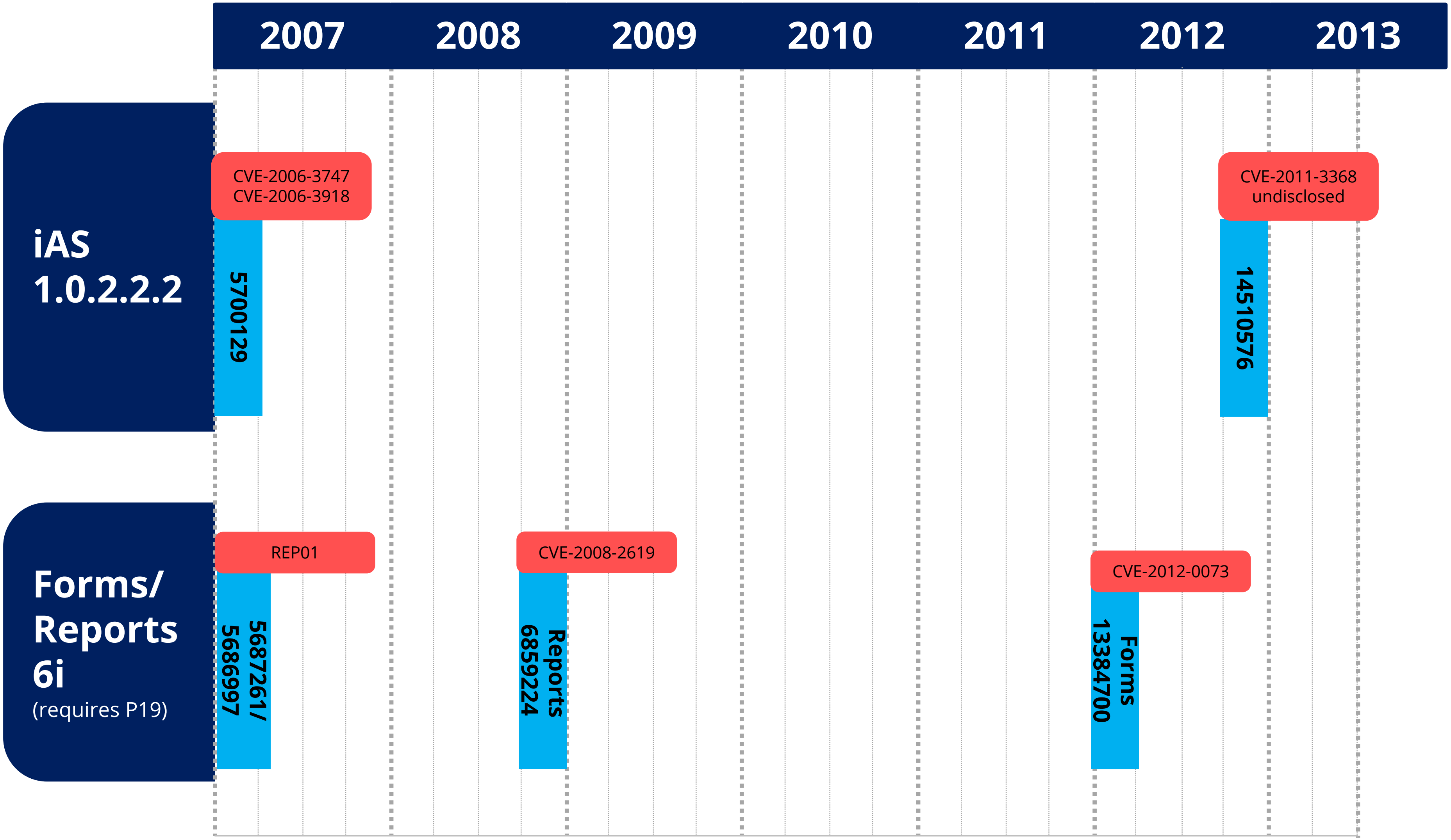
8.0.6.3 Oracle Home

Oracle App Server CPU Risks and Threats

The risk of Oracle EBS application server is mostly related to unpatched security vulnerabilities in the Apache and other web components.

Risk	Description
Unpatched Known Apache 1.3 Vulnerabilities	Limited set of patched Apache 1.3 security vulnerabilities.
Unpatched Unknown Apache 1.3 Vulnerabilities	Apache 1.3 is un-supported and security vulnerabilities are not researched or patched. Discovered vulnerabilities in other Apache versions may be exploitable in Apache 1.3.
Unpatched Forms and Reports Vulnerabilities	Limited set of patched Oracle Forms and Reports vulnerabilities with low impact to Oracle EBS.

Oracle EBS 11i Application Server Patches



2007 2008 2009 2010 2011 2012 2013

iAS 1.0.2.2.2

CVE-2006-3747
CVE-2006-3918

5700129

CVE-2011-3368
undisclosed

14510576

Forms/ Reports 6i
(requires P19)

REP01

5687261/
5686997

CVE-2008-2619

Reports
6859224

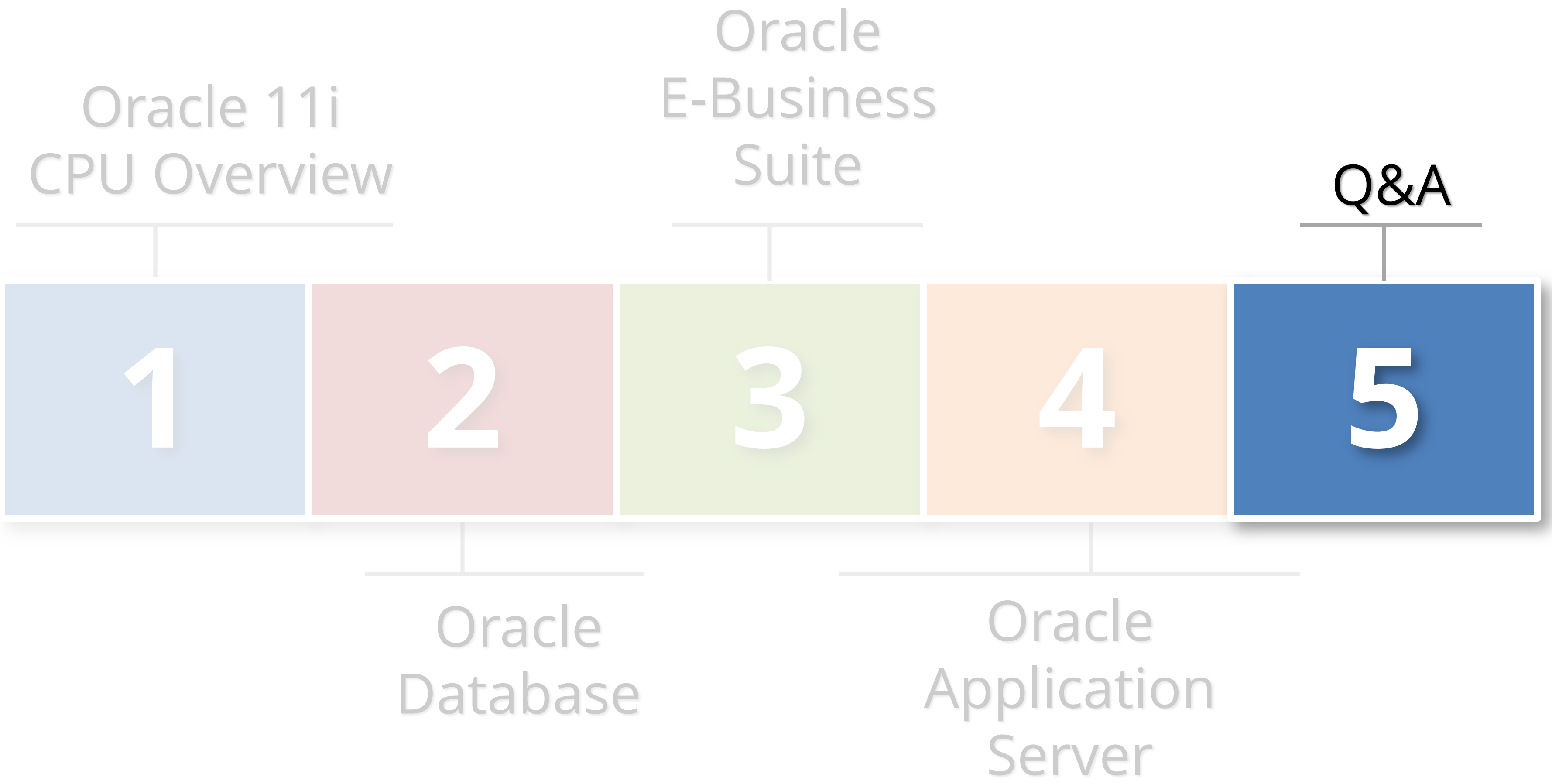
CVE-2012-0073

Forms
13384700

Solutions by Risk for No CPUs

Risk	**Solutions if No CPUs Applied**
Unpatched Known Apache 1.3 Vulnerabilities	#1 – Implement Integrigy's AppDefend #2 – Implement Web Application Firewall
Unpatched Unknown Apache 1.3 Vulnerabilities	
Unpatched Forms and Reports Vulnerabilities	#3 – Limit access to privileged responsibilities

Agenda



1 Oracle 11i CPU Overview

2 Oracle Database

3 Oracle E-Business Suite

4 Oracle Application Server

5 Q&A

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**