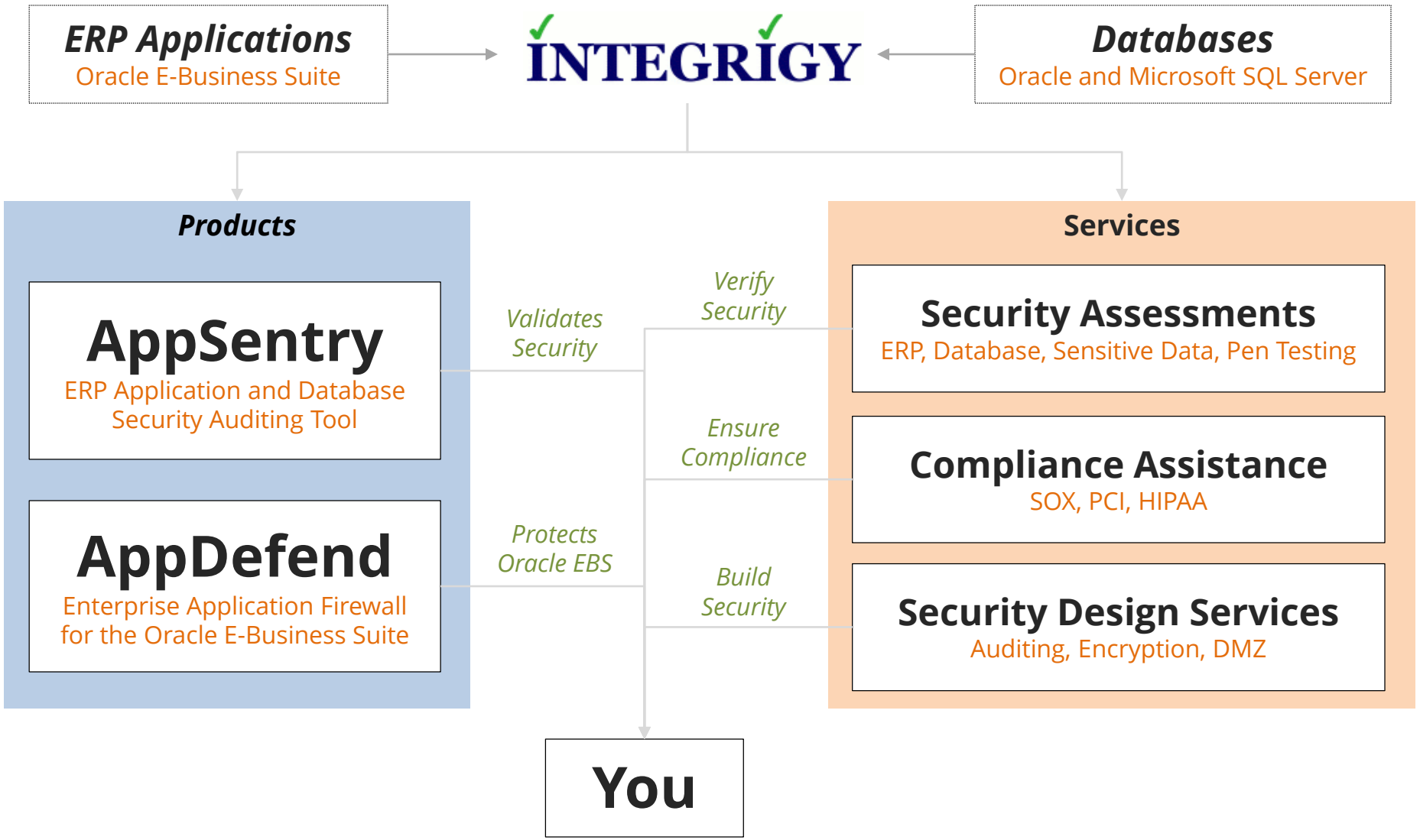

# Security Implications of Oracle Product Desupport

**April 23, 2015**

Stephen Kost
Chief Technology Officer
Integrigy Corporation

# About Integrigy




or

de-support

**de·sup·port** [**dee**-suh-pawrt]

*noun*

1. the state of not being supported.
2. a phenomenon that occurs to Oracle customers.

*verb*

1. to end or remove support.

# Oracle Product Lifetime Support Model

| | |
|---|---|
| **Premier** | ▪ Five years from release<br>▪ Security patches and Critical Patch Updates |
| **Extended** | ▪ Three years additional<br>▪ Security patches and Critical Patch Updates<br>▪ Additional annual fee |
| **Sustaining (desupport)** | ▪ **NO security patches**<br>▪ **NO Critical Patch Updates**<br>▪ Indefinite as long as pay annual maintenance<br>▪ Requires a minimum patch level – usually the terminal patchset or set of patches |

Source: http://www.oracle.com/us/support/lifetime-support/index.html

# Oracle Software Error Correction Support

| | |
|---|---|
| **Oracle Database**<br>**Oracle Fusion Middleware**<br>**Oracle Enterprise Manager** | **MOS Note ID 209768.1** |
| **Oracle E-Business Suite** | **MOS Note ID 1195034.1** |
| **Oracle Lifetime Support** | **http://www.oracle.com/us/support/lifetime-support/index.html** |

# Oracle Database Version Support

| Major Releases | Extended Support End Date | Patchsets | CPU Support End Date |
|---|---|---|---|
| **Oracle 12c R1** | July 2021 | **12.1.0.2** | **TBD** |
| | | **12.1.0.1** | **July 2015** |
| **Oracle 11g R2** | January 2018 | **11.2.0.4** | **January 2018** |
| | | **11.2.0.3** | **July 2015** |
| | | ~~11.2.0.2~~ | ~~January 2013~~ |
| | | ~~11.2.0.1~~ | ~~July 2011~~ |
| **Oracle 11g R1** | August 2015 | **11.1.0.7** | **July 2015** |
| ~~**Oracle 10g R2**~~ | ~~July 2013~~ | ~~10.2.0.5~~ | ~~July 2013~~ |
| ~~**Oracle 10g R1**~~ | ~~January 2012~~ | ~~10.1.0.5~~ | ~~January 2012~~ |

# Oracle E-Business Suite Version Support

| Version | Premier Support End Date | Extended Support End Date (1) | CPU Support End Date |
|---|---|---|---|
| **EBS 12.2** | September 2018 | September 2021 | **July 2021** |
| **EBS 12.1** | December 2016 | December 2019 | **October 2019** |
| ~~**EBS 12.0**~~ | ~~January 2012~~ | ~~January 2015~~ | **January 2015 (2)** |
| **EBS 11.5.10** | ~~November 2010~~ | ~~November 2013~~ | **October 2015 (3)** |
| ~~**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. April 2015 CPU for 12.0 is available for customers with Advanced Support Contracts.
3. 11.5.10 Sustaining support exception through December 2015 provides CPUs.

# Security Implications of Desupport

1. **No security patches or Critical Patch Updates**
2. **No security configuration updates**
3. **No technology stack updates or upgrades**
4. **No major security documentation updates**
5. **No research or validation of submitted security bugs**

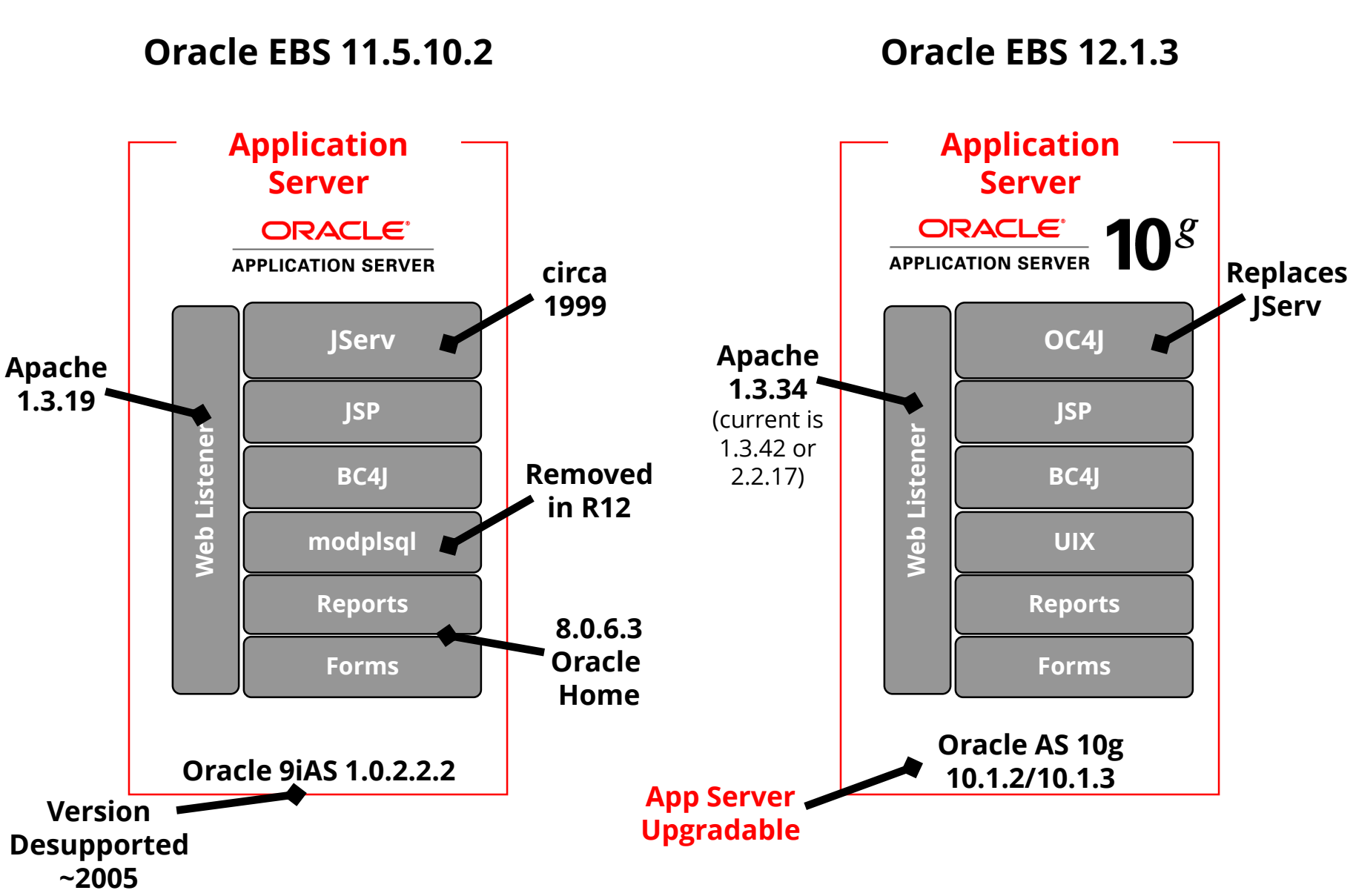
# No Security Configuration Updates

- **State of security changes over time**
  - Hacking techniques and tools evolve
  - HTTP cookie security is a prime example
- **Oracle improves security with tweaks to configuration settings through patches and security patches**
  - Mostly minor and behind the scenes changes, but impact security in a meaningful way
  - Oracle Database privilege changes
  - Oracle E-Business Suite web server configuration

# No Technology Stack Updates or Upgrades

- **Oracle Database**
  - APEX versions not certified
- **Oracle E-Business Suite**
  - New database versions not certified – no security patches for the database
  - Application server security patches not available
  - Apache, Forms, Reports, JServ, and SSL versions for 11.5.10 are ancient – security improvements as well as patches

# 11i/R12 Architecture Differences



# No Security Documentation Updates

- **Oracle Database**
  - Oracle Security Guide not updated

- **Oracle E-Business Suite**
  - Oracle EBS Security Configuration Guide not updated
    - 11i = MOS Note ID 189367.1
    - Last Update September 2011

  - Oracle EBS DMZ Configuration not updated
    - 11i = MOS Note ID 287176.1
    - Last Update October 2011

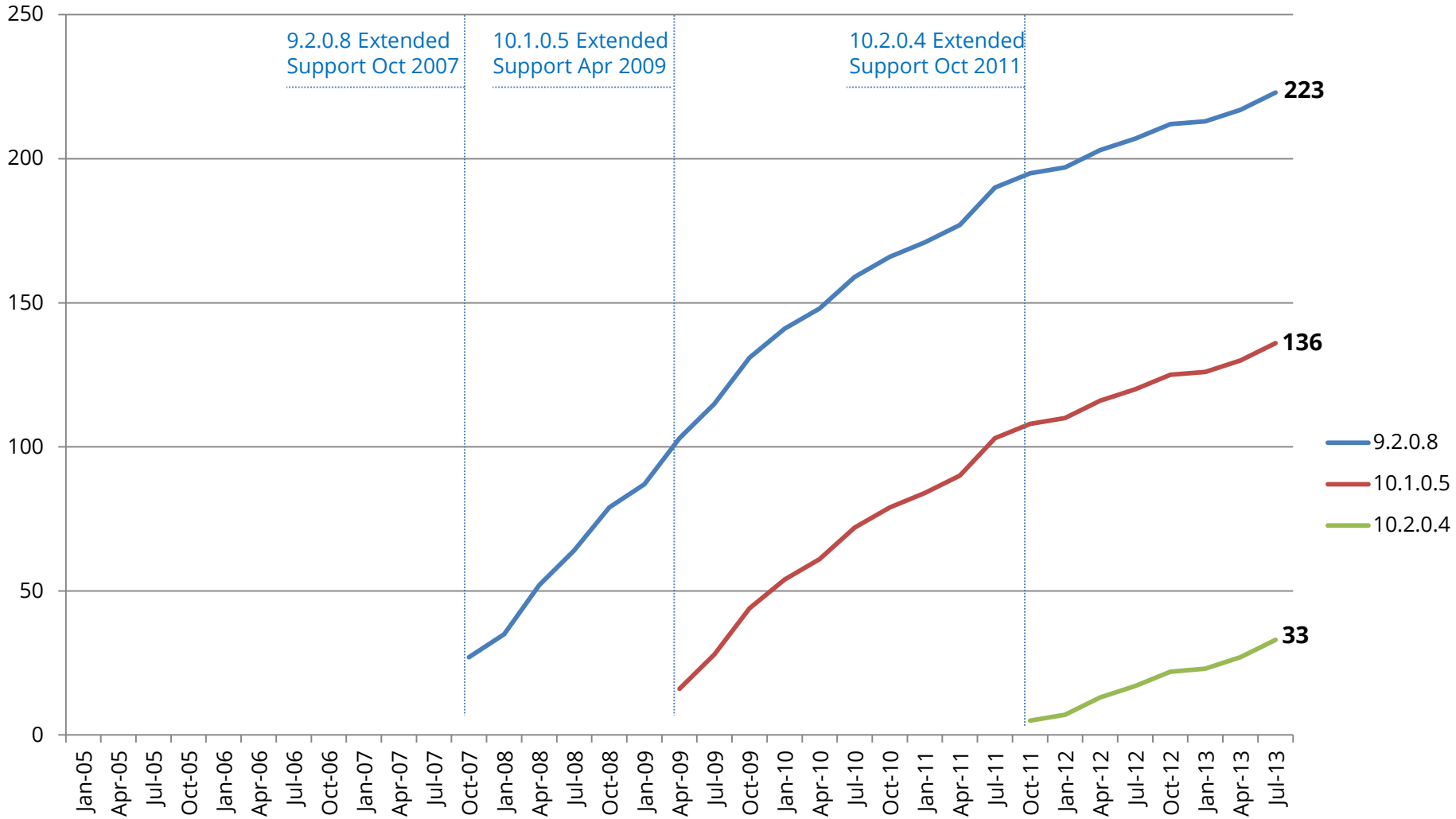
# No Security Vulnerability Research

- **Oracle Software Security Assurance stated policy is not to fix security bugs in desupported products**
  - Researched for supported products
  - Fixed in main code-line first
  - Backported to support products

- **Security bugs may be found in desupported version and never validated by Oracle**
  - Unclear what Oracle's reaction would be to a major vulnerability in a desupported product

# Oracle Database
# Critical Patch Updates

# Cumulative Vulnerabilities per DB Version




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

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

# Solutions by Risk for No CPUs

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

# 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 Firewall**
   - Add-on database security product

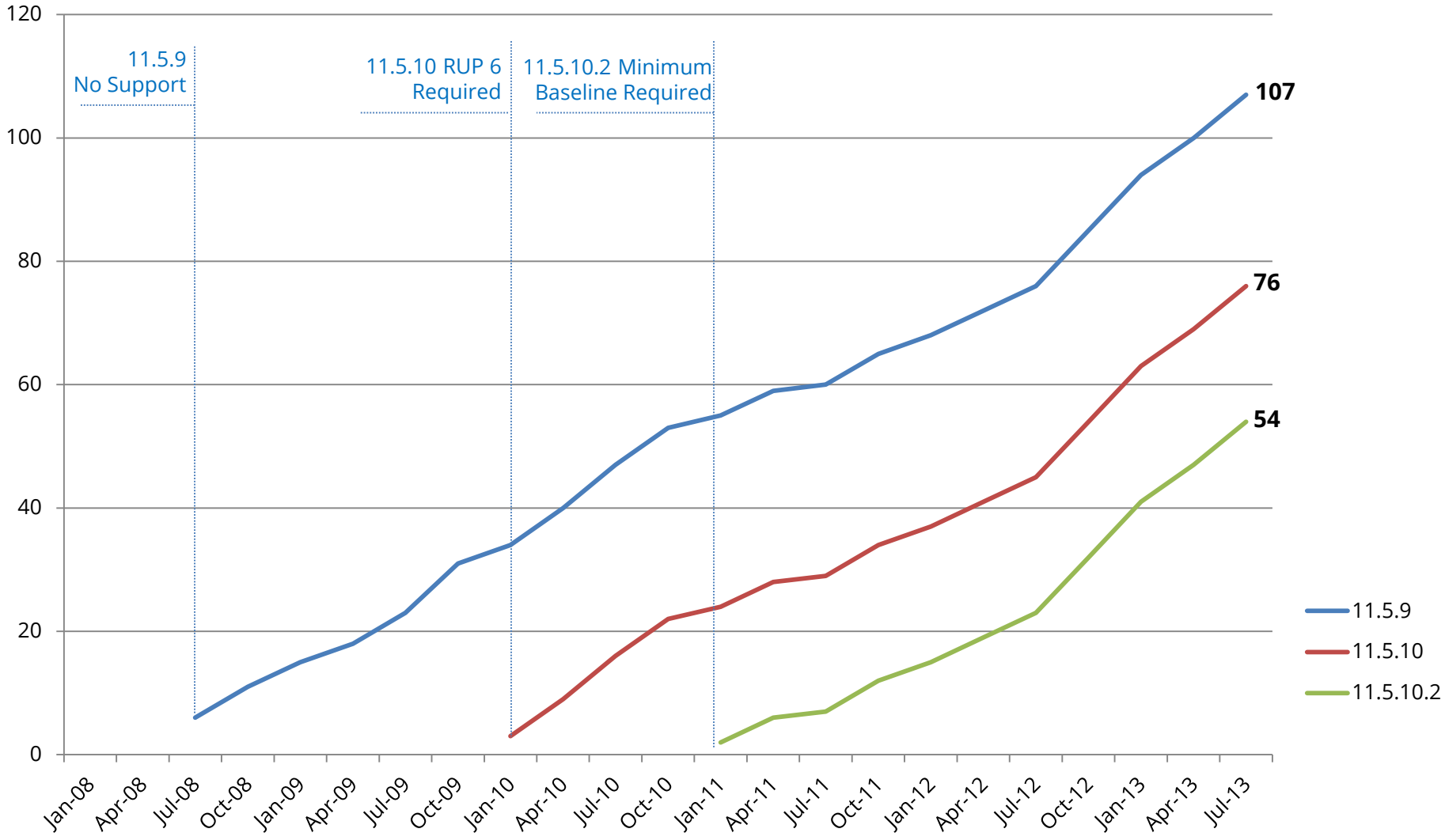
# Oracle E-Business Suite Critical Patch Updates

# 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 |

# Cumulative Vulnerabilities per 11i Version



# 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<br><br>#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

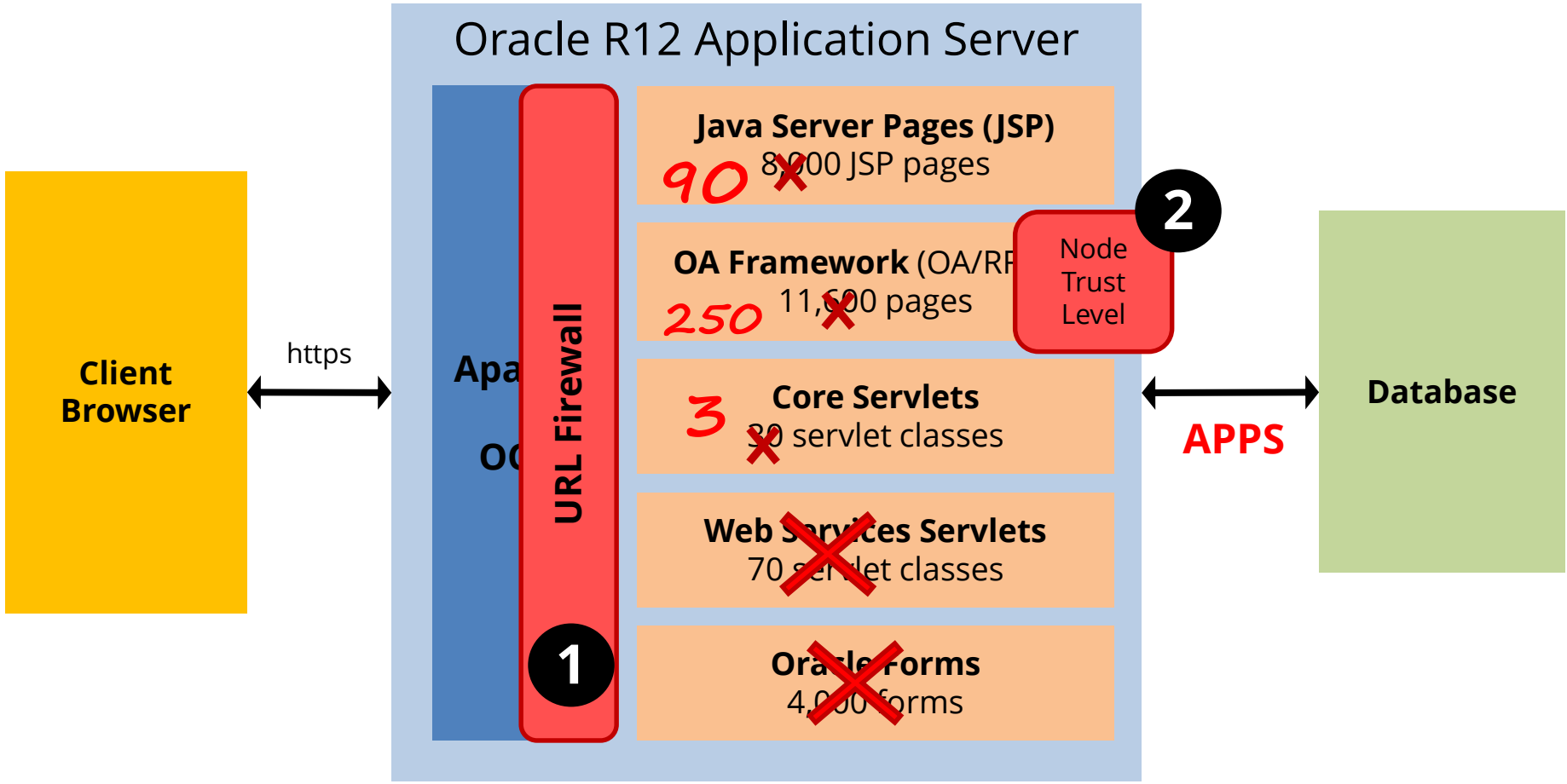
Deploying Oracle E-Business Suite in a DMZ requires a specific and detailed configuration of the application and application server. All steps in the Oracle provided MOS Note must be followed.

**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**