INTEGRIGY

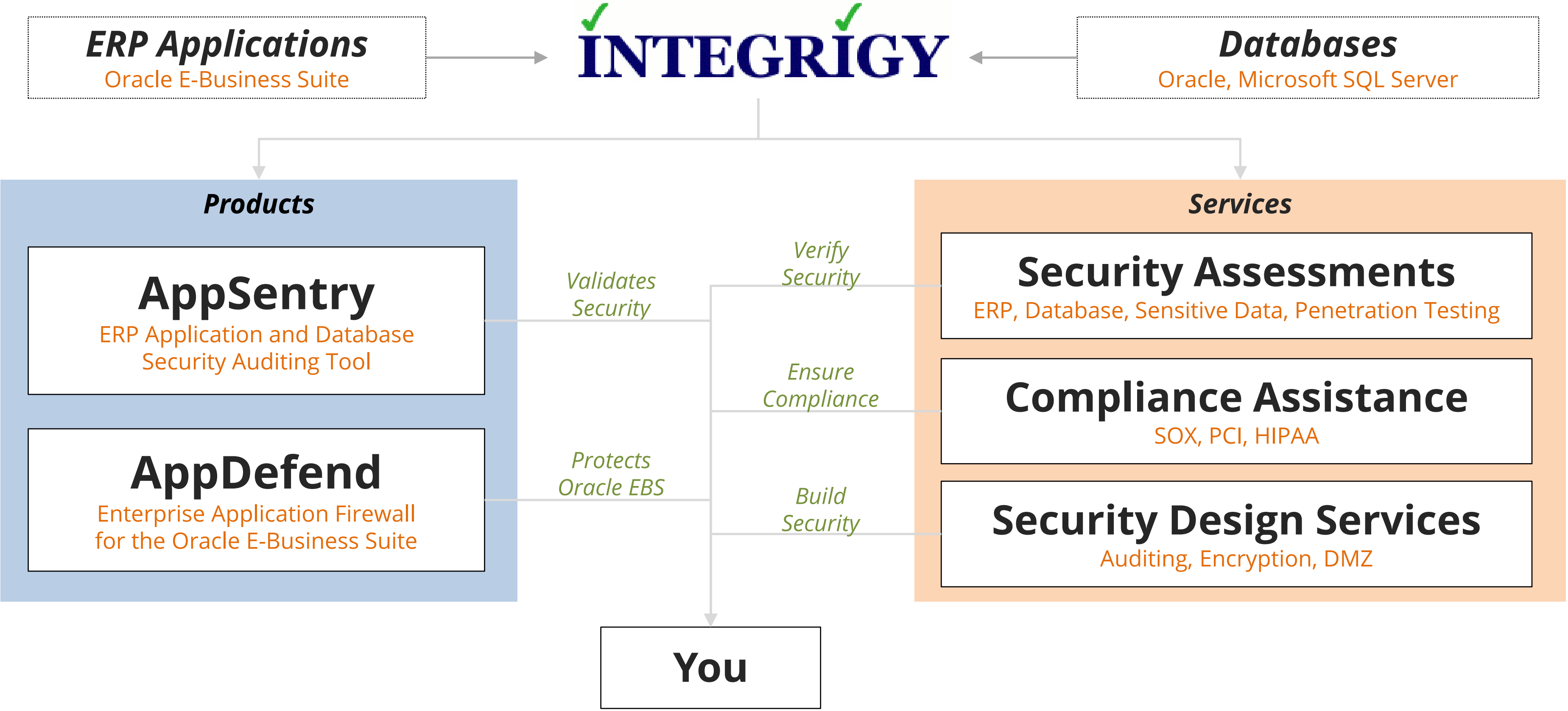
Oracle E-Business Suite
Security Myths

November 13, 2012

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, 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

Verify Security

Ensure Compliance

Build Security

Services

Security Assessments
ERP, Database, Sensitive Data, Penetration Testing

Compliance Assistance
SOX, PCI, HIPAA

Security Design Services
Auditing, Encryption, DMZ

You

Integrigy Published Security Alerts

Security Alert	Versions	Security Vulnerabilities
Critical Patch Update July 2011	11.5.10 – 12.1.x	▪ Oracle E-Business Suite security configuration issue
Critical Patch Update October 2010	11.5.10 – 12.1.x	▪ 2 Oracle E-Business Suite security weaknesses
Critical Patch Update July 2008	Oracle 11g 11.5.8 – 12.0.x	▪ 2 Issues in Oracle RDBMS Authentication ▪ 2 Oracle E-Business Suite vulnerabilities
Critical Patch Update April 2008	12.0.x 11.5.7 – 11.5.10	▪ 8 vulnerabilities, SQL injection, XSS, information disclosure, etc.
Critical Patch Update July 2007	12.0.x 11.5.1 – 11.5.10	▪ 11 vulnerabilities, SQL injection, XSS, information disclosure, etc.
Critical Patch Update October 2005	11.0.x, 11.5.1 – 11.5.10	▪ Default configuration issues
Critical Patch Update July 2005	11.5.1 – 11.5.10 11.0.x	▪ SQL injection vulnerabilities ▪ Information disclosure
Critical Patch Update April 2005	11.5.1 – 11.5.10 11.0.x	▪ SQL injection vulnerabilities ▪ Information disclosure
Critical Patch Update Jan 2005	11.5.1 – 11.5.10 11.0.x	▪ SQL injection vulnerabilities
Oracle Security Alert #68	Oracle 8i, 9i, 10g	▪ Buffer overflows ▪ Listener information leakage
Oracle Security Alert #67	11.0.x, 11.5.1 – 11.5.8	▪ 10 SQL injection vulnerabilities
Oracle Security Alert #56	11.0.x, 11.5.1 – 11.5.8	▪ Buffer overflow in FNDWRR.exe
Oracle Security Alert #55	11.5.1 – 11.5.8	▪ Multiple vulnerabilities in AOL/J Setup Test ▪ Obtain sensitive information (valid session)
Oracle Security Alert #53	10.7, 11.0.x 11.5.1 – 11.5.8	▪ No authentication in FNDFS program ▪ Retrieve any file from O/S

#1

Myth: Oracle E-Business Suite is secure out of the box

#1

Reality: Oracle E-Business Suite requires significant effort to make secure and compliant

For R12 security at a minimum, see My Oracle Support Notes 403537.1, 380490.1, and 376700.1.

Default Database Passwords

- Oracle E-Business Suite database is delivered with up to **300 database accounts**
  - Default passwords (GL = GL)
  - Active
  - **Significant privileges**

Seeded Application Account Responsibilities

Active Application Account	Default Password	Active Responsibilities
ASGADM	WELCOME	▪ SYSTEM_ADMINISTRATOR ▪ ADG_MOBILE_DEVELOPER
IBE_ADMIN	WELCOME	▪ IBE_ADMINISTRATOR
MOBADM	MOBADM	▪ MOBILE_ADMIN ▪ SYSTEM_ADMINISTRATOR
MOBILEADM	WELCOME	▪ ASG_MOBILE_ADMINISTRAOTR ▪ SYSTEM_ADMINISTRATOR
OP_CUST_CARE_ADMIN	OP_CUST_CARE_ADMIN	▪ OP_CUST_CARE_ADMIN
OP_SYSADMIN	OP_SYSADMIN	▪ OP_SYSADMIN
WIZARD	WELCOME	▪ AZ_ISETUP ▪ APPLICATIONS FINANCIALS ▪ APPLICATION IMPLEMENTATION

Application Password Settings

System Profile Options	***11i Default***	***R12 Default***
Signon Password Failure Limit	(null)	10
Signon Password Hard To Guess (1 letter, 1 number, no repeating characters, not username)	No	No
Signon Password Length	5	6
Signon Password No Reuse	(null)	(null)
Signon Password Case	insensitive	insensitive

Signon Password settings must be changed to meet organization’s password policy

Oracle EBS Password Decryption

- Oracle EBS end-user application passwords stored **encrypted**, not **hashed**
  - Account passwords stored in **FND_USER** table
  - Procedure to decrypt passwords well documented and published on the Internet
  - Google: oracle applications password decryption

- Secure hashing of passwords is **optional** and must be enabled by DBA
  - **Not enabled by default even in R12**
  - See Integrigy whitepaper for recommendations

Securing the Configuration

Adhere to the Oracle Best Practices for securely configuring the Oracle E-Business Suite – written by Integrigy

189367.1 *Secure Configuration Guide for Oracle E-Business Suite* ***11i***

403537.1 *Secure Configuration Guide for Oracle E-Business Suite* ***R12***

Securing the DMZ Configuration

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 Metalink 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*

Other Oracle Security Notes

11i: A Guide to Understanding and Implementing SSL for Oracle Applications/Enabling SSL in Release 12	123718.1 **11i** 376700.1 **R12**
Enabling SSL with Oracle Application Server 10g and the E-Business Suite	340178.1
Encrypting EBS 11i Network Traffic using Advanced Security Option (also for R12)	391248.1
Oracle Applications Credit Card Encryption for 11i	338756.1
Using Transparent Data Encryption (TDE) with the E-Business Suite	403294.1 **11i** 732764.1 **R12** 828229.1 **R12**
Using Oracle Database Vault with Oracle E-Business Suite Releases 11i and 12	950018.1
Configuring Oracle Connection Manager With Oracle E-Business Suite Release 12	558959.1

#2

Myth: Oracle EBS is secure if you implement most items in the Secure Configuration Guide

#2

Reality: All items in the Secure Configuration Guide are a base minimum and additional steps are required

Significant Security Risks and Threats

Risks and Threats ▪ examples	**1** DB Pass	**2** App Pass	**3** Direct Access	**4** App Sec Design	**5** Extern App	**6** Patch Policy	**7** SQL Forms	**8** Change Control	**9** Audit	**10** Pass Control
1. Sensitive data loss (data theft) ▪ Bulk download via direct access ▪ Bulk download via indirect access	🔴		🔴		🔴	🟡		🟡		
2. Direct entering of transactions (fraud) ▪ Update a bank account number ▪ Change an application password	🔴		🔴	🔴	🟡		🔴	🔴	🟡	🔴
3. Misuse of application privileges (fraud) ▪ Bypass intended app controls ▪ Access another user’s privileges		🔴		🔴	🟡	🔴			🟡	🔴
4. Impact availability of the application ▪ Wipe out the database ▪ Denial of service (DoS)	🔴	🟡	🔴		🟡	🔴	🟡	🟡		

Top 10 Security Vulnerabilities

1. Default Database Passwords
2. Default Application Passwords
3. Direct Database Access
4. Poor Application Security Design
5. External Application Access Configuration
6. Poor Patching Policies and Procedures
7. Access to SQL Forms in Application
8. Weak Change Control Procedures
9. No Database or Application Auditing
10. Weak Application Password Controls

Other Oracle Security Notes

11i: A Guide to Understanding and Implementing SSL for Oracle Applications/Enabling SSL in Release 12	123718.1 **11i** 376700.1 **R12**
Enabling SSL with Oracle Application Server 10g and the E-Business Suite	340178.1
Encrypting EBS 11i Network Traffic using Advanced Security Option (also for R12)	391248.1
Oracle Applications Credit Card Encryption for 11i	338756.1
Using Transparent Data Encryption (TDE) with the E-Business Suite	403294.1 **11i** 732764.1 **R12** 828229.1 **R12**
Using Oracle Database Vault with Oracle E-Business Suite Releases 11i and 12	950018.1
Configuring Oracle Connection Manager With Oracle E-Business Suite Release 12	558959.1

#3

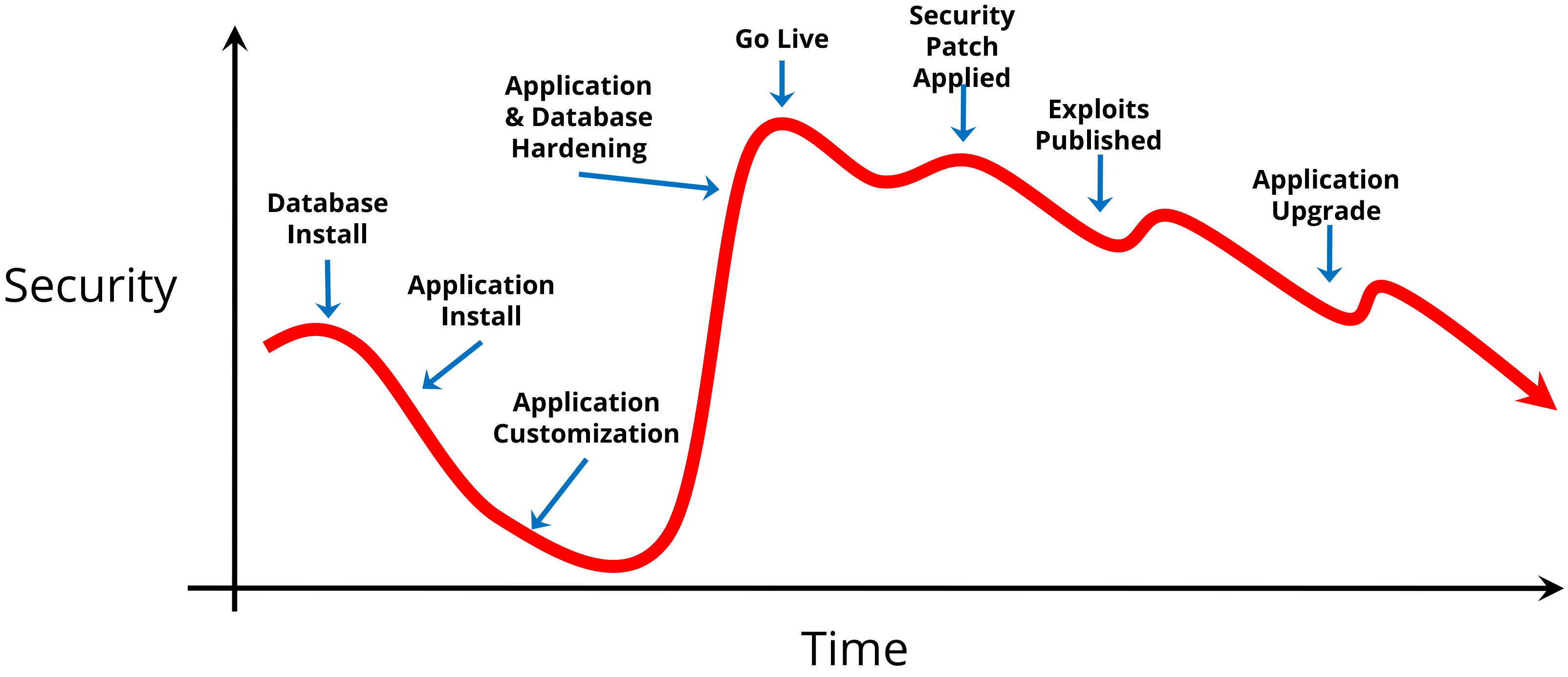
Myth: We hardened Oracle EBS at go-live – we are secure today

#3

Reality: Oracle EBS security decays over time and steps must be taken routinely to validate security

Application Security Decay

Application security decays over time due to complexity, usage, application changes, upgrades, published security exploits, etc.



Default Oracle Password Statistics

Database Account	Default Password	Exists in Database %	Default Password %
SYS	CHANGE_ON_INSTALL	100%	3%
SYSTEM	MANAGER	100%	4%
DBSNMP	**DBSNMP**	**99%**	**52%**
OUTLN	**OUTLN**	**98%**	**43%**
MDSYS	MDSYS	77%	18%
ORDPLUGINS	ORDPLUGINS	77%	16%
ORDSYS	ORDSYS	77%	16%
XDB	CHANGE_ON_INSTALL	75%	15%
DIP	DIP	63%	19%
WMSYS	WMSYS	63%	12%
CTXSYS	**CTXSYS**	**54%**	**32%**

* Sample of 120 production databases

Database Accounts Added During Upgrade

- A new database account is added for each new product module during an upgrade
- The default password for each new account is the username

CA, DDR, DNA, DPP, FTP, GMO, IBW, INL, IPM, ITA, JMF, MTH, PFT, QPR, RRS,

How to Check Database Passwords

- Use Oracle’s **DBA_USERS_WITH_DEFPWD**
  - Limited set of accounts
  - Single password for each account

- **Command line tools** (orabf, etc.)
  - Difficult to run – command line only

- **AppSentry**
  - Checks all database accounts
  - Uses passwords lists - > 1 million passwords
  - Allows custom passwords

R12 Application Users Added

- New application accounts from 12.0.0 onward
  - INDUSTRY DATA
  - ORACLE12.0.0
  - ORACLE12.1.0
  - ORACLE12.2.0
  - ORACLE12.3.0
  - ORACLE12.4.0
  - ORACLE12.5.0
  - ORACLE12.6.0
  - ORACLE12.7.0
  - ORACLE12.8.0
  - ORACLE12.9.0

- All are active accounts with invalid passwords

#4

Myth:

(i) Your IT Security team is protecting Oracle EBS

(ii) Your DBAs are protecting Oracle EBS

#4

Reality: Securing Oracle EBS is hard and requires a focused effort from a multidisciplinary team

Oracle DBAs, Oracle project team, IT Security, and Internal Audit must work together to make Oracle EBS secure and compliant

Organizational Misalignment

Oracle E-Business Suite technical security often not effectively handled in most organizations and **“falls between the cracks.”**

- **Database and Application Administrators**
  Priority is performance, maintenance, and uptime

- **IT Security**
  No understanding of database or Oracle EBS security

- **Internal Audit**
  Focused on application controls, segregation of duties

What should you do?

- **Ensure the application is securely configured**

  Work with DBAs to understand what has been done and not done

- **Understand how data is accessed and protected**

  Learn what sensitive data is in Oracle EBS, who accesses it, and what is done to protect it

- **Obsess over security of the external configuration**

  External access to the application should keep you up at night

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-JUL-09 08.50.30.021401 AM	APPLY	10.2.0.4	CPUJul2009
16-OCT-10 07.18.57.042620 AM	APPLY	10.2.0.4	CPUOct2010
30-OCT-10 06.42.55.108783 AM	UPGRADE	11.1.0.7.0	Upgraded from 10.2.0.4.0

What CPU Level is this database patched to?

A. January 2007 B. January 2009 C. January 2010 D. October 2010

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-JUL-09 08.50.30.021401 AM	APPLY	10.2.0.4	CPUJul2009
16-OCT-10 07.18.57.042620 AM	APPLY	10.2.0.4	CPUOct2010
30-OCT-10 06.42.55.108783 AM	UPGRADE	11.1.0.7.0	Upgraded from 10.2.0.4.0

What CPU Level is this database patched to?

A. January 2007 [✓ **B. January 2009**] **C. January 2010** **D. October 2010**

#5

Myth: When installing or upgrading, the latest Oracle Critical Patch Updates (CPU) are already included

#5

Reality: For both the database and Oracle EBS, only the latest CPU at time of release is included

Almost always have to install the latest CPU when doing a fresh installation or upgrade to both the database and Oracle EBS

Critical Patch Updates 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

EBS Version	Included CPU
12.0.6	October 2008
12.1.1	April 2009
12.1.2	October 2009
12.1.3	January 2011

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

#6

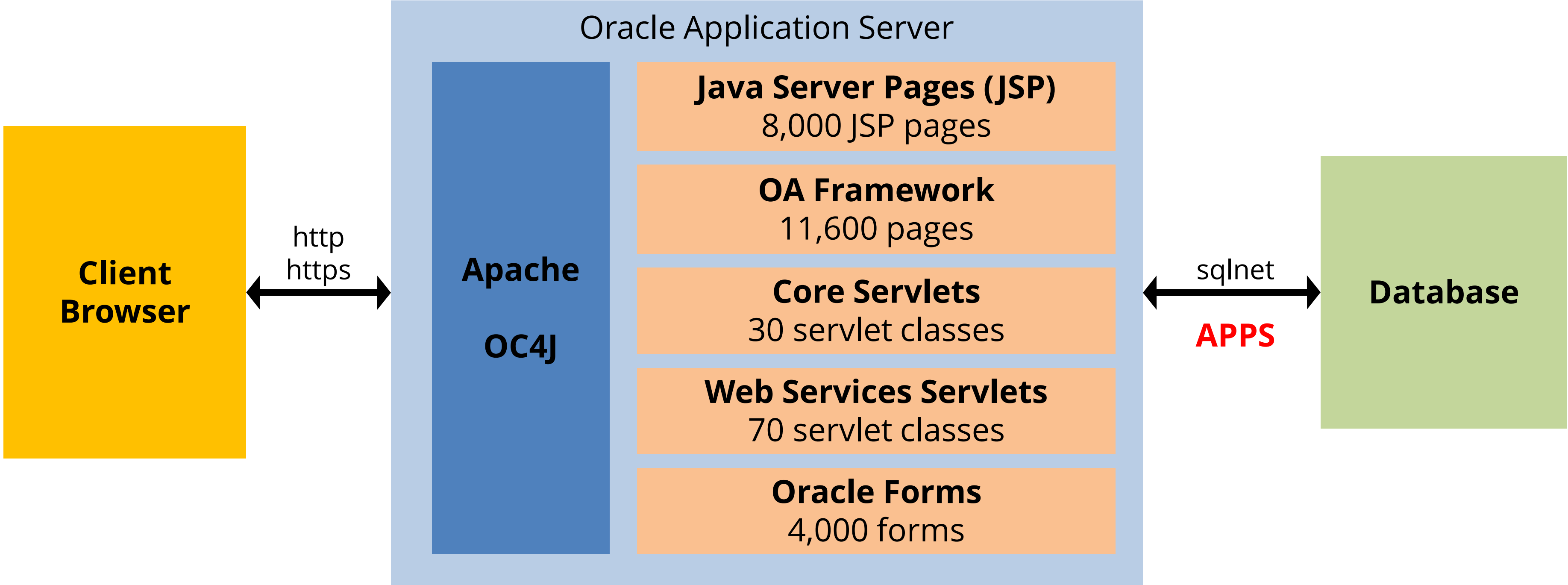
Myth: The only modules running are what you have installed, configured, and licensed

#6

Reality: Every Oracle EBS module is installed and parts can be accessed even if not configured or licensed

Significant security impact as Oracle EBS has a massive footprint

Oracle EBS R12 Web Footprint



- Oracle EBS installs all modules (250+) and **all web pages** for every application server
- All web pages access the database using the **APPS** database account

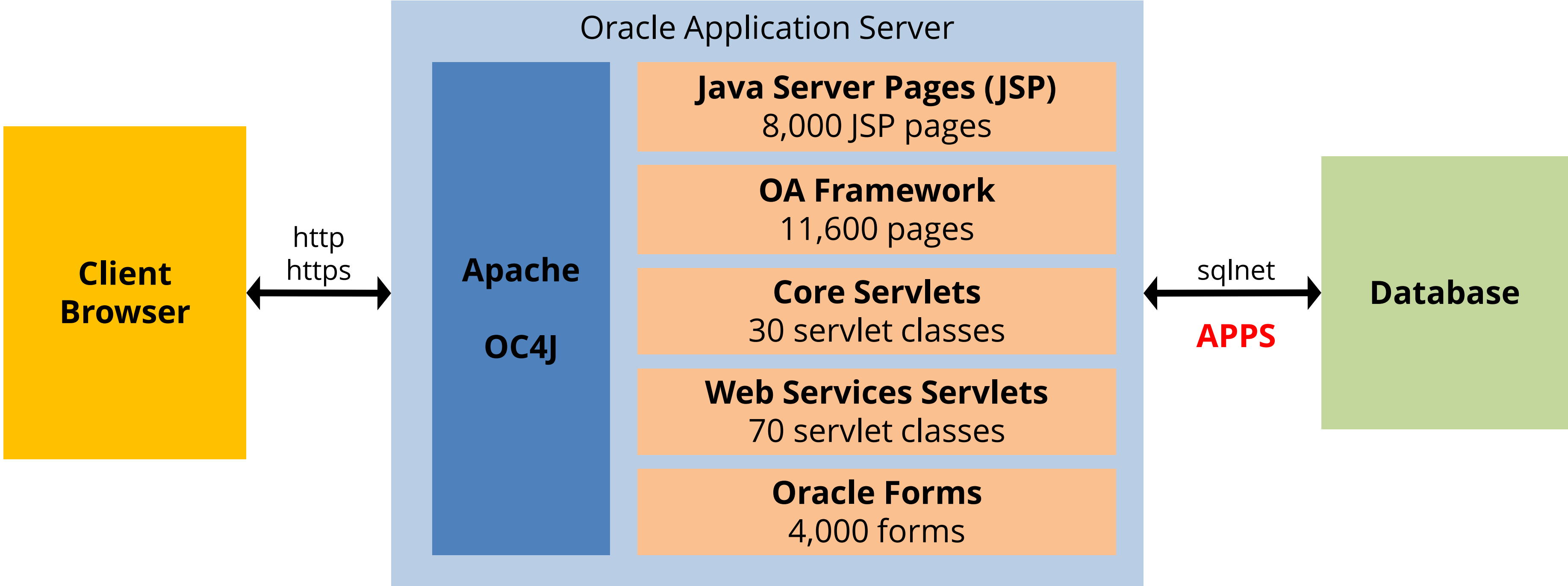
#7

Myth: Oracle EBS Critical Patch Updates (CPU) don’t have to be installed if I don’t use those modules

#7

Reality: Since every module is installed and can be potentially accessed, every CPU must be installed

Oracle EBS R12 Web Footprint



- Oracle EBS installs all modules (250+) and **all web pages** for every application server
- All web pages access the database using the **APPS** database account

#8

Myth: Our network security will protect Oracle EBS from web attacks when deployed externally

We have routers, firewalls, intrusion protection systems, web application firewalls, etc. in place to protect Oracle EBS

#8

Reality: Network security layers are not aware or tuned for Oracle EBS

Firewalls, intrusion protection systems, and web application firewalls have few if any rules or protection for Oracle EBS

Web Application Firewall Shortcomings

- **Must be heavily customized for Oracle EBS**
  Rules, application profiles, and learning must be developed, tuned, and tested by you

- **Unable to block unused Oracle EBS modules**
  Due to the complexity of the Oracle naming and design, very difficult to implement blocking of EBS modules with WAF rules

- **Significant cost, effort, and skill required to deploy**
  WAFs are usually an appliance that must be deployed and the learning curve for configuring and operating an enterprise WAF is steep

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

- **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)

How to Check the External Configuration

1. Review DMZ web architecture
   - SSL
   - Network firewall
   - Reverse proxy
   - Web application firewall
   - Load balancing and caching
2. Perform a penetration test?
3. Review URL firewall configuration
4. Configuration Review - Manual
   - Review 8 major configuration steps
5. Configuration Review - AppSentry
   - Automates checking 6 of 8 major configuration steps

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**