

The Manager's Guide to Securing the Oracle E-Business Suite

June 2, 2012

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

Agenda

Security
Challenges

Protecting Data

Q&A

1

2

3

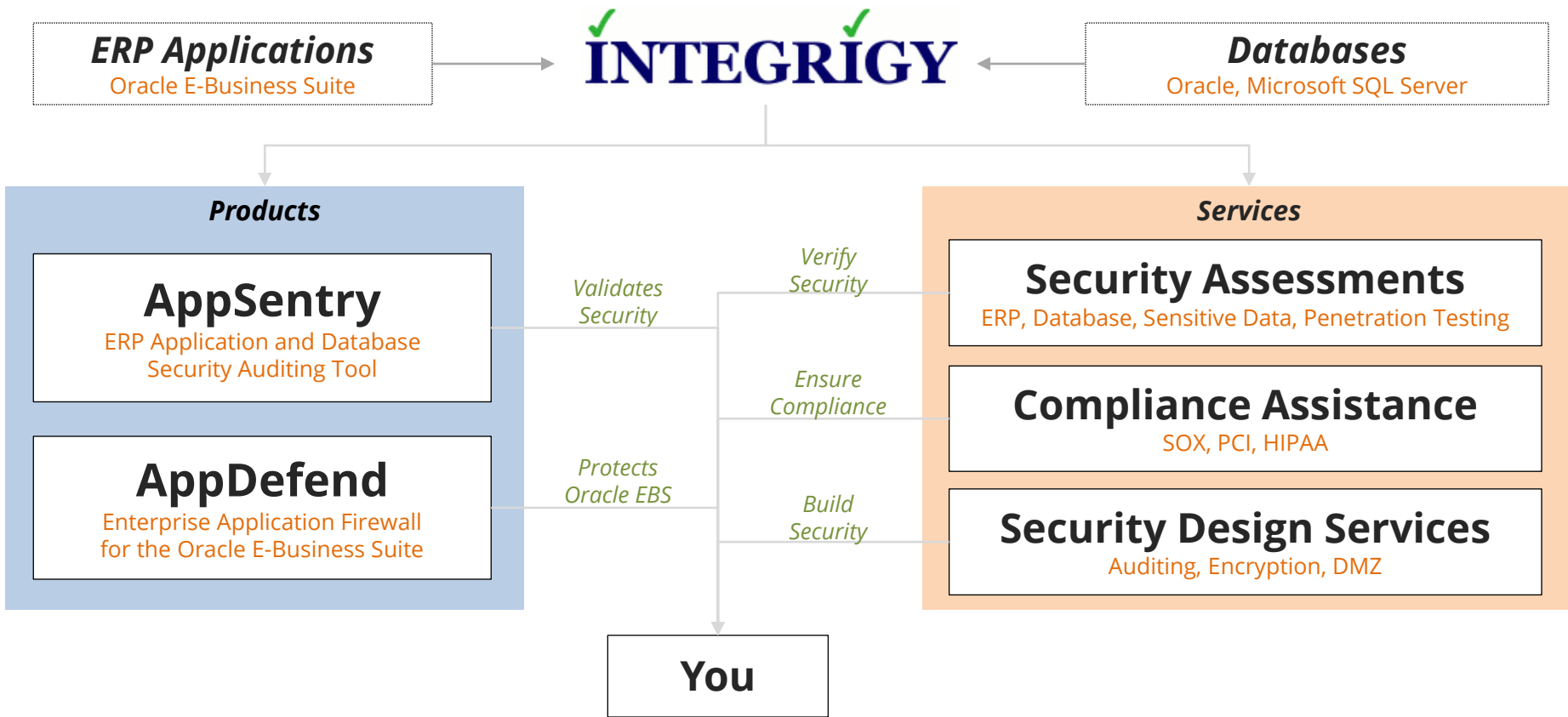
4

5

Configuration

External Access

About Integrigy



Agenda

Security
Challenges

Protecting Data

Q&A

1

2

3

4

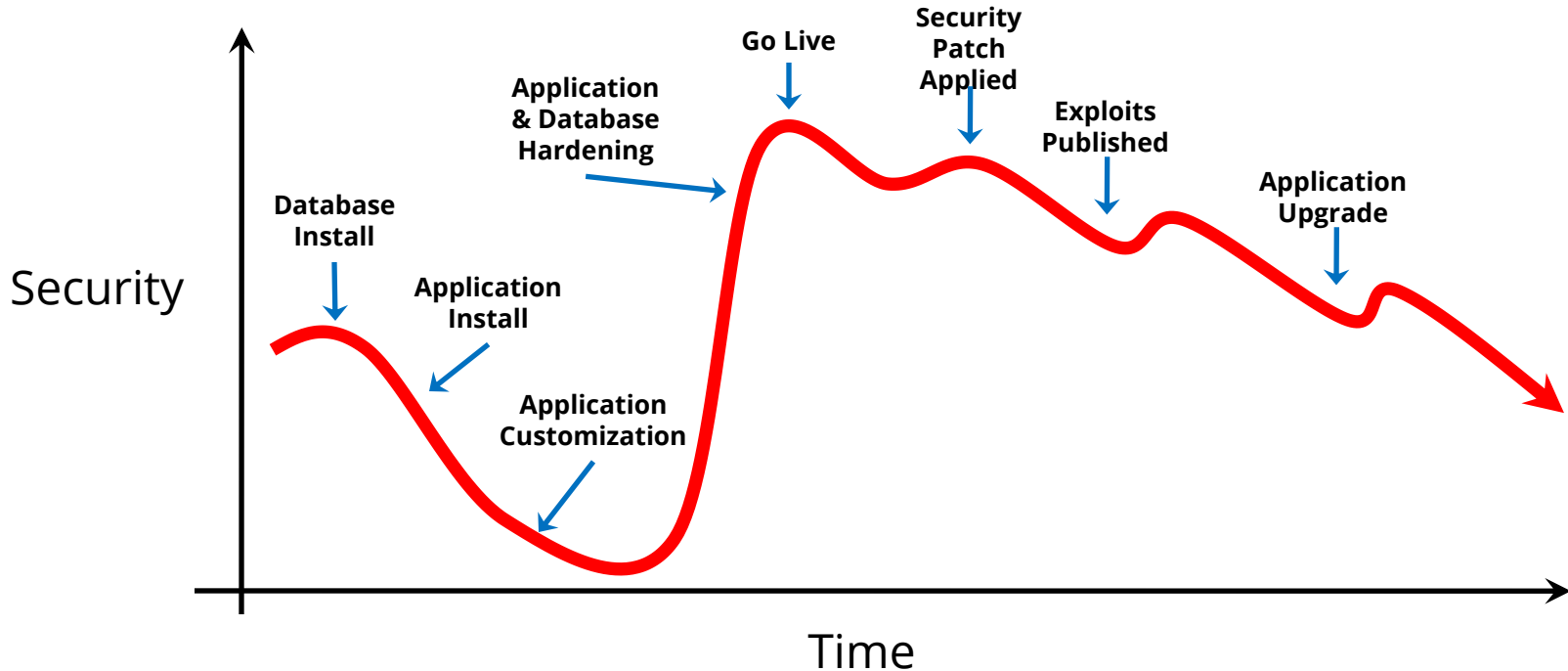
5

Configuration

External Access

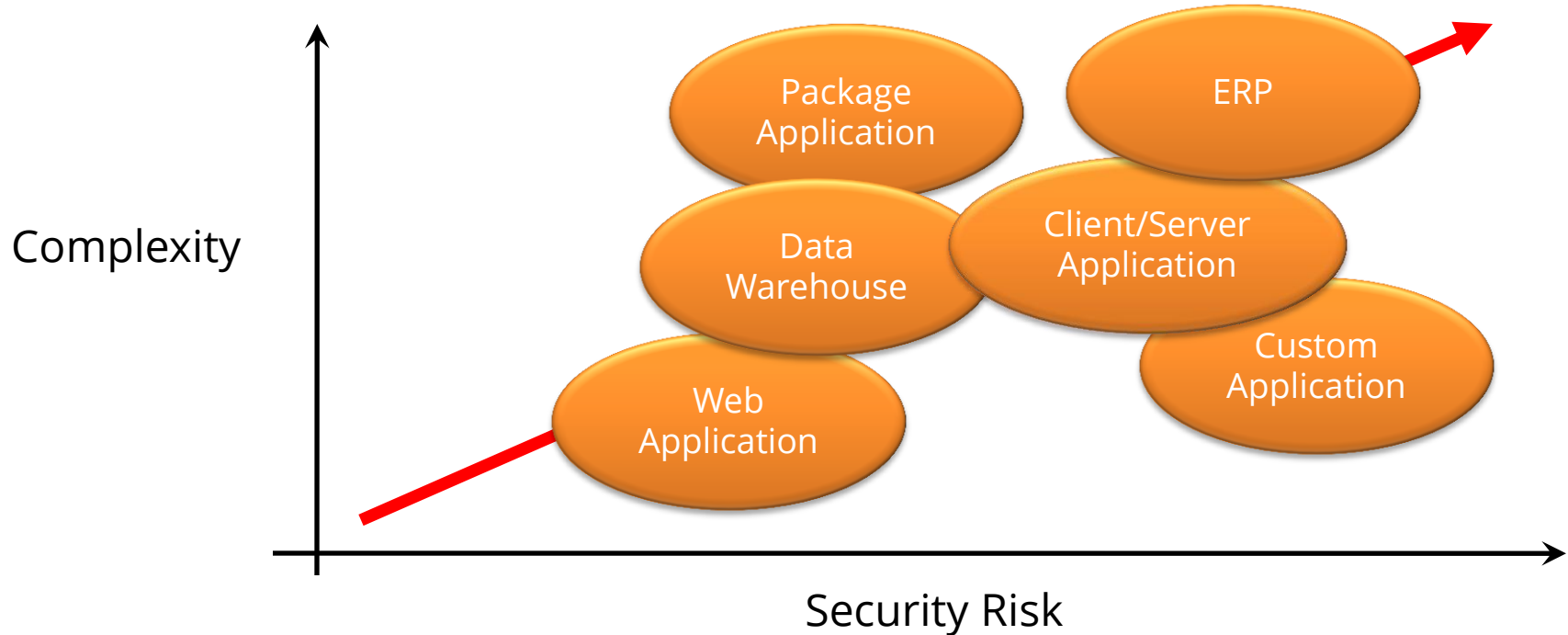
Application Security Decay

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



Complexity and Security are Opposed

The more complex a database and application environment are, the less secure the entire environment will be.



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

Top 10 Oracle EBS Security Risks

- 1 **Default Database Passwords**
- 2 **Default Application Passwords**
- 3 **External Application Access Configuration**
- 4 **Direct Database Access**
- 5 **Poor Application Security Design**
- 6 **Poor Patching Policies and Procedures**
- 7 **Lack of encryption on sensitive data**
- 8 **Weak Change Control Procedures**
- 9 **No Database or Application Auditing**
- 10 **Weak Application Password Controls**

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 Data Encryption	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)										

Overall - What should a manager 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

Agenda

Security
Challenges

1

Protecting Data

2

3

4

Q&A

5

Configuration

External Access

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***

Default Database Passwords

Oracle E-Business Suite database is delivered with up to **300 database accounts**

- Default passwords (GL = GL)
- Active
- **Significant privileges**

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

Seeded Application Account Responsibilities

Active Application Account	Default Password	Active Responsibilities
ASGADM	WELCOME	<ul style="list-style-type: none">▪ SYSTEM_ADMINISTRATOR▪ ADG_MOBILE_DEVELOPER
IBE_ADMIN	WELCOME	<ul style="list-style-type: none">▪ IBE_ADMINISTRATOR
MOBADM	MOBADM	<ul style="list-style-type: none">▪ MOBILE_ADMIN▪ SYSTEM_ADMINISTRATOR
MOBILEADM	WELCOME	<ul style="list-style-type: none">▪ ASG_MOBILE_ADMINISTRAOTR▪ SYSTEM_ADMINISTRATOR
OP_CUST_CARE_ADMIN	OP_CUST_CARE_ADMIN	<ul style="list-style-type: none">▪ OP_CUST_CARE_ADMIN
OP_SYSADMIN	OP_SYSADMIN	<ul style="list-style-type: none">▪ OP_SYSADMIN
WIZARD	WELCOME	<ul style="list-style-type: none">▪ AZ_ISETUP▪ APPLICATIONS FINANCIALS▪ APPLICATION IMPLEMENTATION

Oracle EBS Password Controls

1. Password Profile Options

- Length, reuse, case, and failure limit are System Profile Options
- Password expiration time set for individual accounts

2. Password operational procedures

- Initial passwords and password resets
- Default methods in 11i and R12 weak
- Improved in R12 with User Management (UMX)

3. Secure Password Storage

- Allows decryption of account passwords
- Not enabled by default

Configuration - What should a manager do?

- ❖ **Ensure the secure configuration has been applied**
Talk with DBAs to determine the status and completeness
- ❖ **Verify the secure configuration is complete**
Oracle E-Business Suite is complex and “the devil is in the details” with many settings and options
- ❖ **Periodically review and assess the configuration**
Patches, upgrades, etc. introduce security issues

Oracle Critical Patch Updates

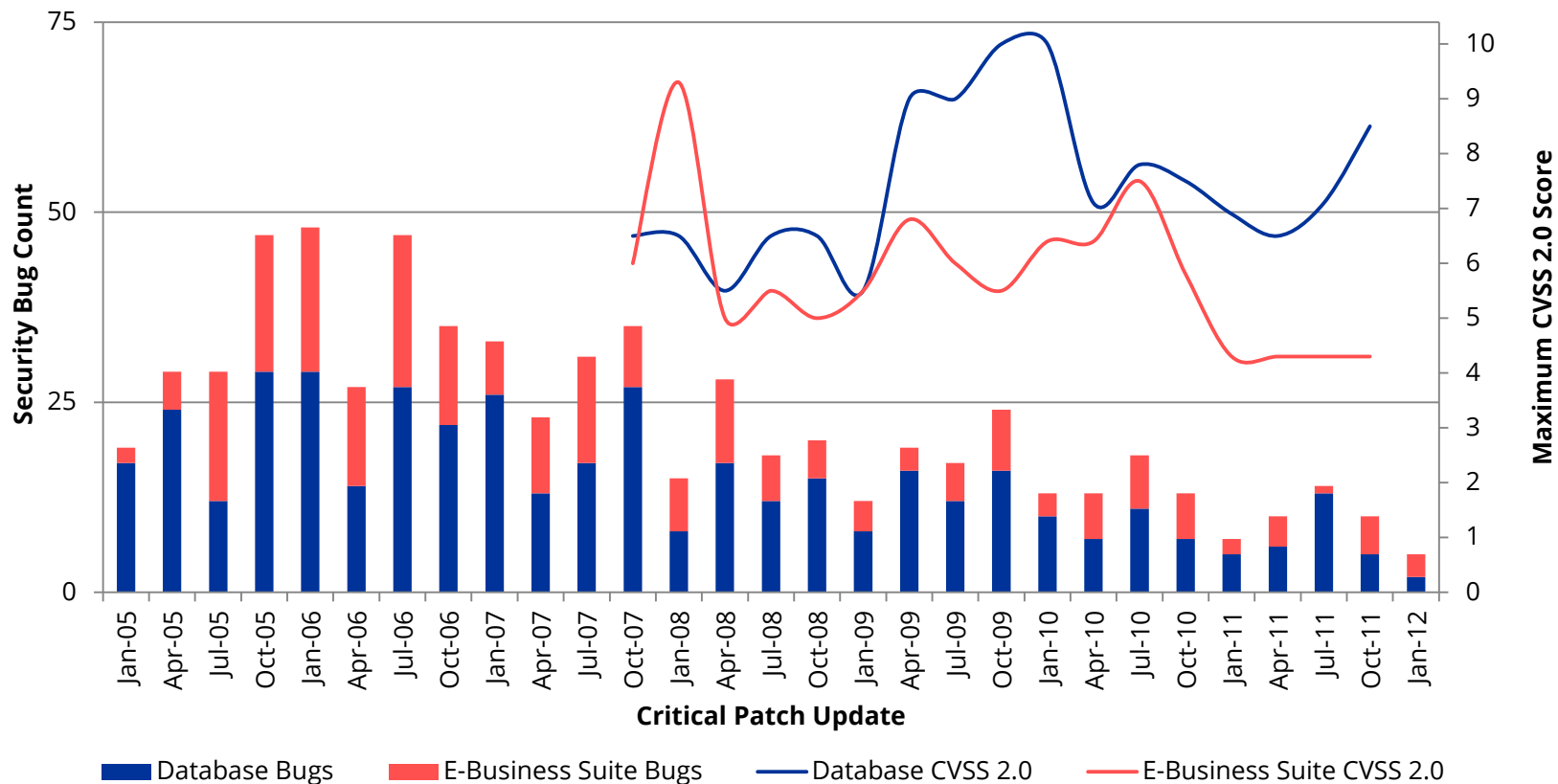
Fixes for security bugs in all Oracle products

- Released quarterly on a fixed schedule
- Tuesday closest to the **17th** day of January, April, July and October
- Next CPUs = **July 17, 2012** and **October 16, 2012**

Thirty CPUs released to date starting with January 2005

- 1,397 security bugs fixed (average is 48 bugs per CPU)
- 433 bugs in the Oracle Database
- 236 bugs in the Oracle E-Business Suite

Oracle Security Bugs per Quarter



CPU Patches - What should a manager do?

- ❖ **Work with the business to prioritize security patches**
Management must support patching effort and downtime
- ❖ **Follow standard patching procedure for CPU patches**
Database patches require minimal testing and application patches need standard regression testing
- ❖ **Ensure security patches are included with all upgrades**
All database and application upgrades should include CPU patches

Agenda

Security
Challenges

Protecting Data

Q&A

1

2

3

4

5

Configuration

External Access

Where is Sensitive Data in Oracle EBS?

Credit Card Data	iby_security_segments (encrypted) ap_bank_accounts_all oe_order_headers_all aso_payments oks_k_headers_* oks_k_lines_* iby_trxn_summaries_all iby_credit_card
Social Security Number (National Identifier) (Tax ID)	per_all_people_f hr_h2pi_employees ben_reporting ap_suppliers ap_suppliers_int po_vendors_obs
Bank Account Number	ap_checks_all ap_invoice_payments_all ap_selected_invoice_checks_all
Protected Health Information (PHI)	Order Management Accounts Receivables Human Resources

Where else might be Sensitive Data?

- **Custom tables**
 - Customizations may be used to store or process sensitive data
- **“Maintenance tables”**
 - DBA copies tables to make backup prior to direct SQL update
 - hr.per_all_people_f_011510
- **Interface tables**
 - Credit card numbers are often accepted in external applications and sent to Oracle EBS
- **Interface files**
 - Flat files used for interfaces or batch processing
- **Log files**
 - Log files generated by the application (e.g., iPayment)
- **Oracle EBS Flexfields**
 - It happens – very hard to find

Credit Card Number Encryption

- **Use the Oracle E-Business Suite encryption**
 - Application-level encryption
 - Better solution than other technologies such as Oracle Transparent Data Encryption (TDE)
- **Metalink Note ID 338756.1, Patch 4607647**
 - Consolidates card numbers into IBY_SECURITY_SEGMENTS table
 - Encrypts card numbers in IBY_SECURITY_SEGMENTS
 - Uniform masking of card numbers
 - Significant functional pre-requisites (11.5.10.2)

Protecting Sensitive Data

- **Access to sensitive data by generic accounts**
 - Granularity of database privileges, complexity of data model, and number of tables/views make it difficult to create limited privilege database accounts
 - Must use individual database accounts with roles limiting access to data along with other security
- **All sensitive data must be scrambled in all non production databases**
 - Must periodically review database for instances of non-scrambled data as often in custom, interface, and temporary tables

Protecting Data - What should a manager do?

- ❖ **Know what data your have and where it is**

Require DBAs and development to maintain data inventory

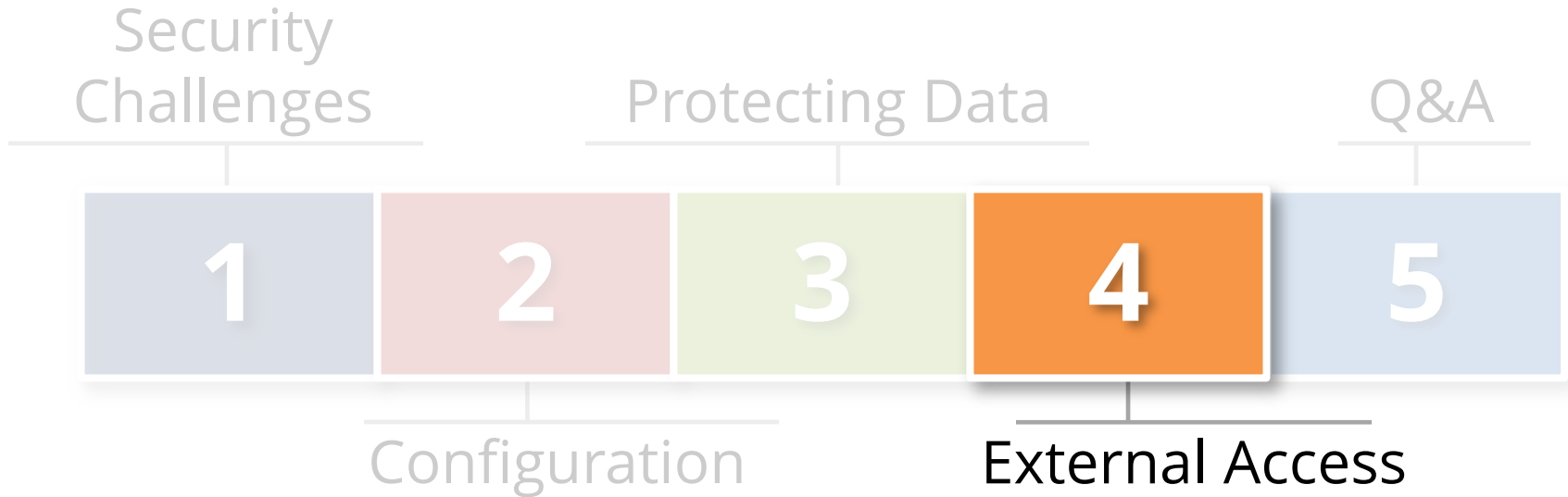
- ❖ **Be vigilant regarding direct database access**

Work to eliminate read accounts (APPS_READ) and direct database access whenever possible

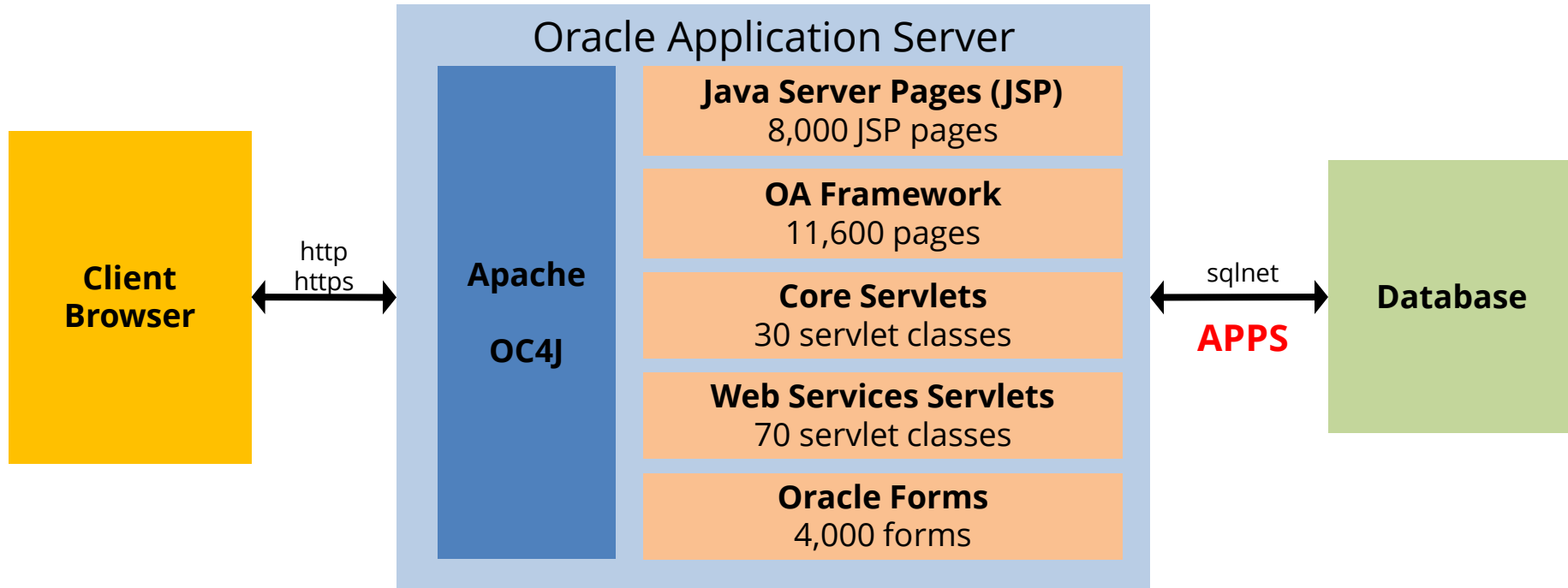
- ❖ **Ask questions regarding data access**

Be sure actual data access equates to business reasons

Agenda

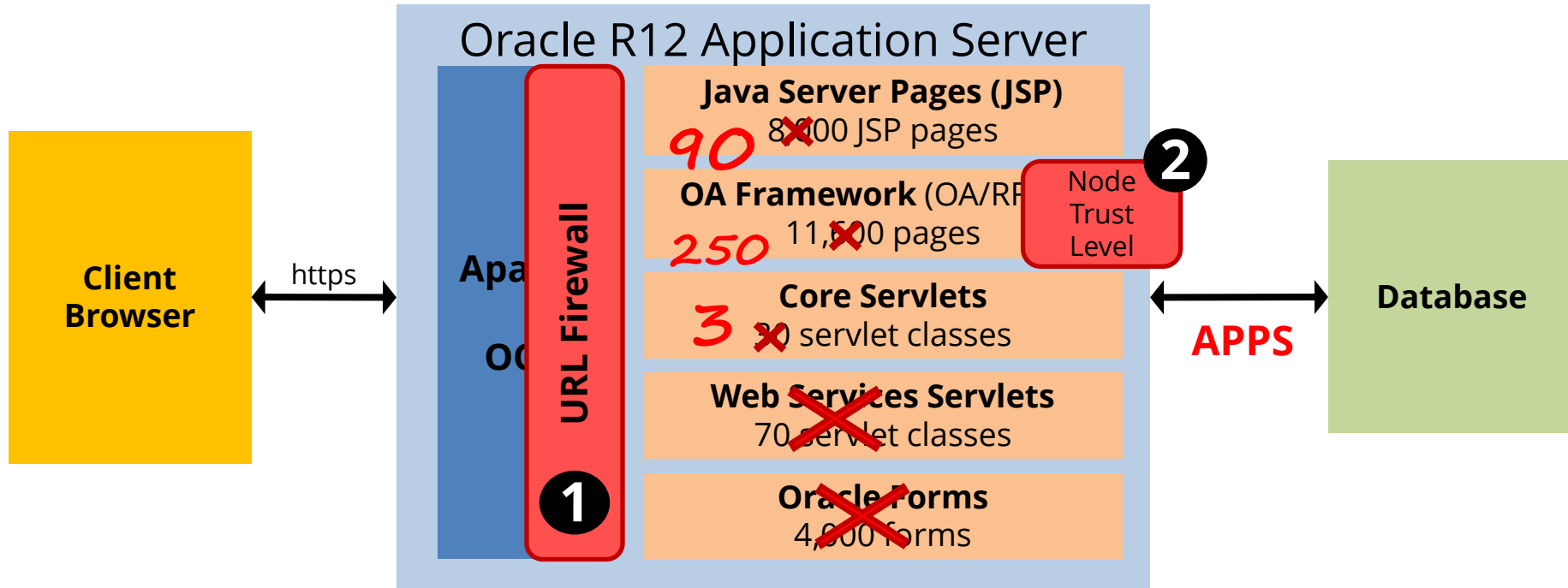


External Access Configuration



- 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

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.

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)

Oracle EBS DMZ Oracle Support 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 My Oracle Support (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*

External DMZ - What should a manager do?

- ❖ **Ensure the DMZ configuration has been applied**

Talk with DBAs to determine the status and completeness

- ❖ **Verify the DMZ configuration is complete**

The DMZ configuration is very specific and every step must be followed exactly – very prone to errors

- ❖ **Periodically review and assess the configuration**

Perform external assessments or penetration tests

Agenda

Security
Challenges

1

Protecting Data

2

3

4

Q&A

5

Configuration

External Access

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