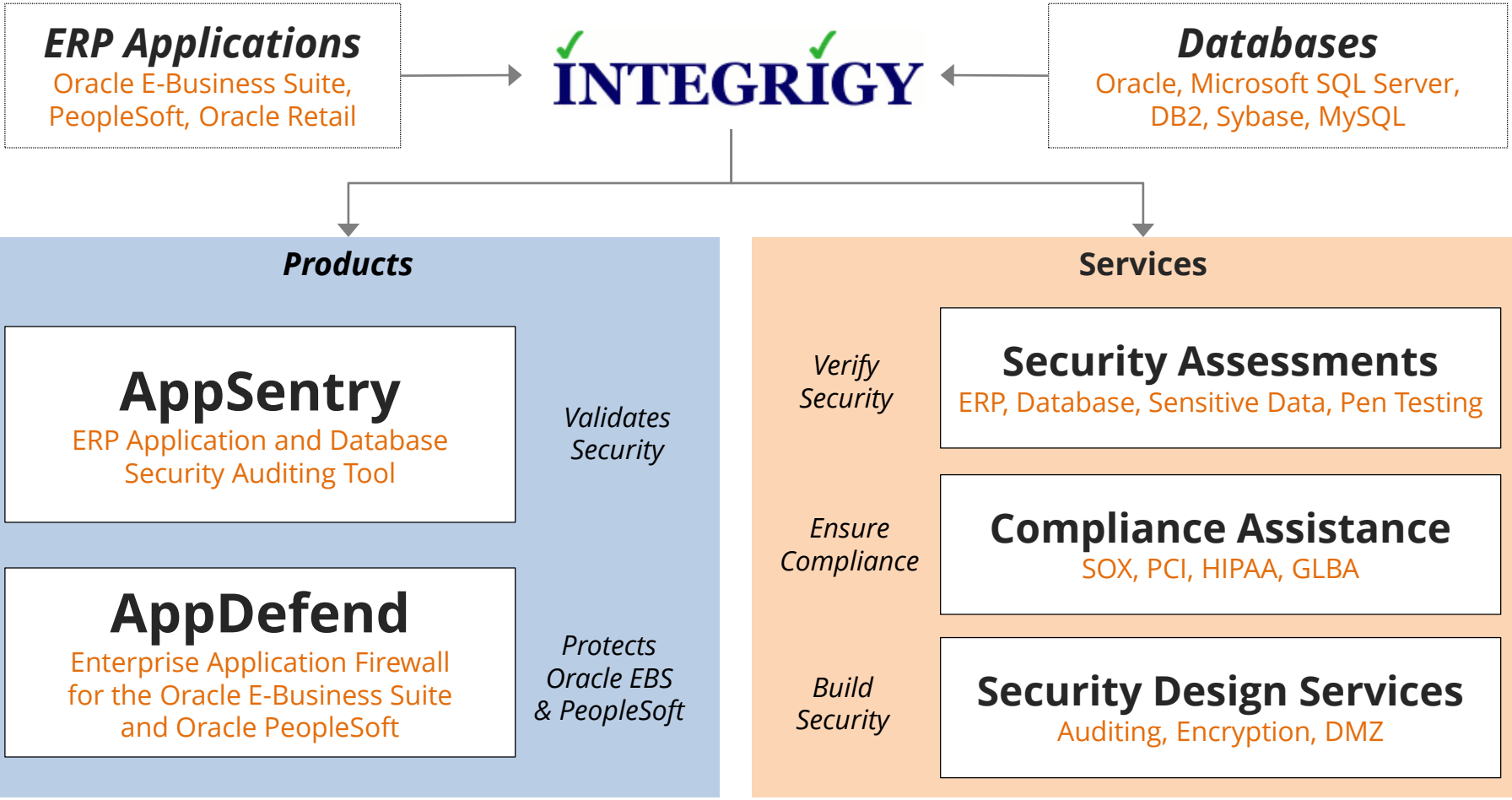
Top 10 Oracle E-Business Suite Security Risks

May 2, 2019

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

About Integrigy



Top 10 Oracle E-Business Suite Security Risks

- ***How was the list of Top 10 security risks developed?***
  - From Integrigy's on-site and remote security assessments of large Oracle E-Business Suite environments over the past 2 years
  - From the Integrigy Research Team's in-depth analysis of the entire Oracle E-Business Suite technology stack including application, database, and application server

- ***What is the selection criteria for the Top 10 security risks in a Oracle E-Business Suite Environment?***
  - What can be pragmatically addressed or should be discussed
  - Risk of PeopleSoft sensitive data loss or information disclosure

Top 10 Security Vulnerabilities

1. Default Database Passwords
2. APPLSYSPUB password not changed
3. URL Firewall not enabled for DMZ
4. Missing security patches
5. EBS password hashing not enabled
6. Direct database access by users
7. SSL/TLS not configured
8. Weak controls for privileged accounts
9. No Database or Application Auditing
10. Sensitive data not encrypted at rest

Significant Security Risks and Threats

Risks and Threats ▪ examples	**1** DB Pass	**2** APPL SYS PUB	**3** URL Firewall DMZ	**4** Missing Security Patches	**5** EBS Password Hashing	**6** Direct DB Access	**7** No SSL/TLS	**8** Priv Accounts	**9** No db-app Audit	**10** Sensitive Data Encrypt
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 ▪ Denial of service (DoS)	✸	✸	✸	✸	✸			✸		

1 Default Database Passwords

- **Oracle E-Business Suite database is delivered with up to 300 database accounts**
  - Default passwords (GL = GL)
  - Active
  - Significant privileges
- **Database accounts are often created with default or weak passwords**
  - Standard Oracle accounts (DBSNMP, CTXSYS, etc.) until 12c created with default passwords by default
  - Named users frequently assigned passwords like WELCOME1

1 Default Database Passwords Risk

- **Risk of a database account with a default password is based on how well-known the account is –**
  1. Standard Oracle Database accounts (DBSNMP, etc.)
  2. Oracle EBS standard account names (APPLSYS, GL, AP, AR, etc.)
  3. Third-party software (OEM, Vertex, etc.)
  4. Custom database accounts (organizational specific)

- **An attacker will –**
  - Scan the internal network for Oracle Databases
  - Use tools like nmap to test for default passwords
  - Most tools have between 250 to 1,500 known Oracle database accounts and passwords

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

How to Check Database Passwords

1. **Use Oracle's DBA_USERS_WITH_DEFPWD**
   - Limited set of accounts
   - Single password for each account
2. **Command line tools (orabf, etc.)**
   - Difficult to run – command line only
3. **AppSentry**
   - Checks all database accounts
   - Uses passwords lists - > 1 million passwords
   - Allows custom passwords

2 APPLSYSPUB with default password

- **Oracle EBS installs default database account APPLSYSPUB with the default password of PUB**
- **APPLSYSPUB has only limited privileges –**
  - System privileges = CREATE SESSION
  - Object privileges = Limited set of SELECT, INSERT, UPDATE, EXECUTE
  - Periodically verify no other privileges have been granted – Oracle EBS Secure Configuration Console will check APPLSYSPUB privileges
- **Oracle sees no need to change the password**
- **When Oracle Database Critical Patch Update security patches are not applied, any database account can potentially compromise the entire database due to vulnerabilities in PUBLIC packages**

3 Oracle EBS DMZ MOS Notes

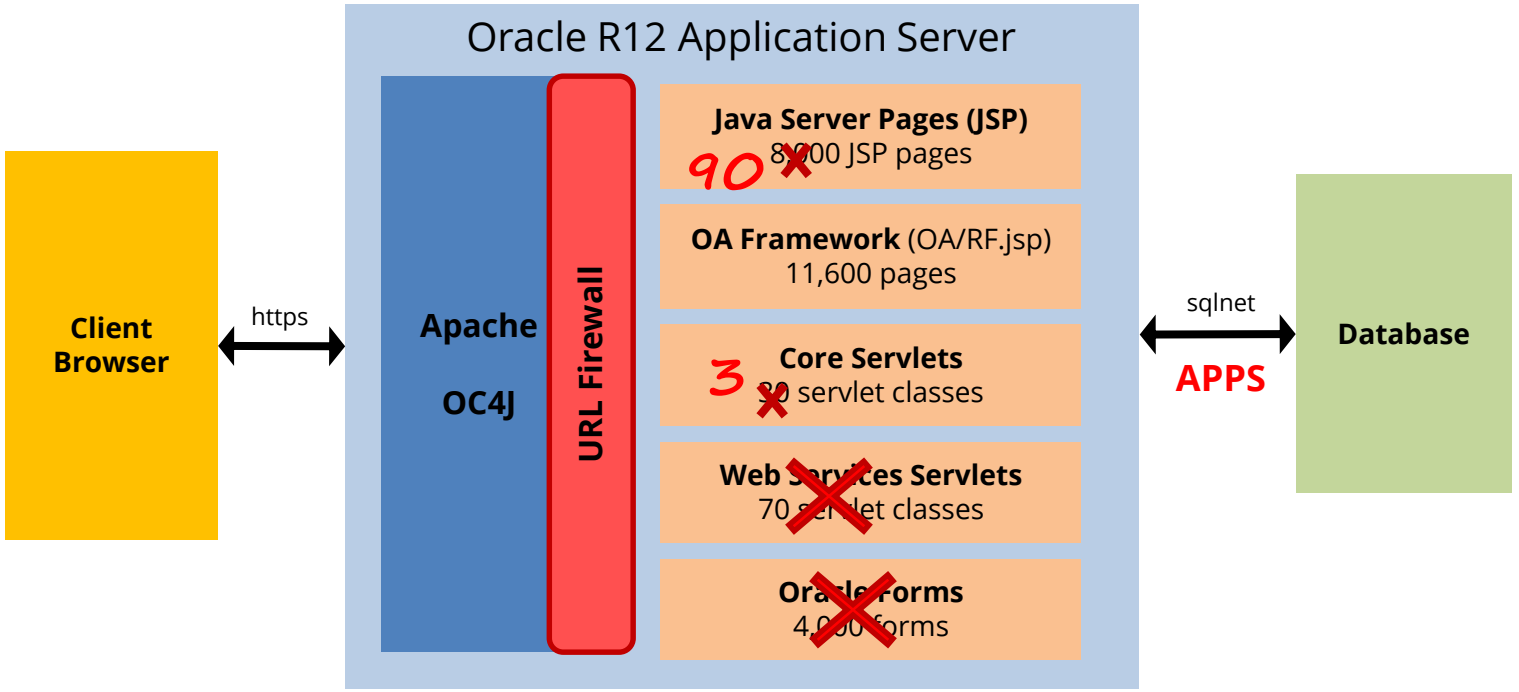
Deploying Oracle E-Business Suite in a DMZ requires a specific and detailed configuration of the application and application server. **All steps** in the Oracle provided MOS Note must be followed.

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

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

DMZ Step Appendix E – URL Firewall – MANDATORY

The Oracle E-Business Suite URL Firewall is a **whitelist** of allowed JSP pages and servlets. Allows all OA Framework pages. Configure using **url_fw.conf**.



How to Check the External Configuration

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

4 No Security Patching

Oracle E-Business Suite security vulnerabilities fixed between January 2005 and April 2019

740

Oracle E-Business Suite and Critical Patch Updates

Oracle E-Business Suite	▪ Cumulative patches per release (12.1, 12.2)
Oracle Database	▪ Patch Set Updates – see quarterly MOS note
Fusion Middleware (12.1)	▪ Security Patch Update – see quarterly MOS note
WebLogic (12.2)	▪ Patch Set Updates – see quarterly MOS note
Java	▪ Point upgrades

Database Versions and CPU Support

Major Releases	Extended Support End Date	Patchsets	CPU Support End Date
Oracle 12c R1	July 2021	**12.1.0.2**	**July 2021**
		12.1.0.1	~~July 2016~~ (extended from July 2015)
Oracle 11g R2	December 2020	**11.2.0.4**	**October 2020** (extended from October 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~~

See MOS Note *Release Schedule of Current Database Releases* (Doc ID 742060.1)

Oracle E-Business Suite Version Support

Version	Premier Support End Date	Extended Support End Date (1)	CPU Support End Date	References MOS Note ID
EBS 12.2	December 2030	TBD	**October 2030**	Lifetime Support
EBS 12.1	December 2021	N/A	**October 2021**	1495337.1
~~**EBS 12.0**~~	~~January 2012~~	~~January 2015~~	**January 2015**	
~~**EBS 11.5.10**~~	~~November 2010~~	~~November 2013~~	**January 2016 (2, 3)**	1596629.1
~~**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. After January 2016, CPUs are available for customers with Advanced Support Contracts – see MOS Note ID 1596629.1.
3. 11.5.10 Sustaining support exception through January 2016 provides CPUs – see MOS Note ID 1596629.1.

Oracle EBS Extended Support Requirements

12.2	▪ EBS 12.2.3 ▪ R12.AD.C.DELTA.10 ▪ R12.TXK.C.DELTA.10
12.1	▪ Basically 12.1.3 ▪ Application Server 10.1.3.5 ▪ R12.ATG_PF.B.DELTA.3 ▪ R12.FWK.B.DELTA.5
12.0	▪ EBS 12.0.6 ▪ Application Server 10.1.2.3 & 10.1.3.5 ▪ Java 6
11.5.10	▪ ATG RUP 6 or ATG RUP 7

Source: MOS Note ID 1195034.1 - Oracle E-Business Suite Error Correction Support Policy (V.5 – January 2015)

Oracle E-Business Suite and Critical Patch Updates

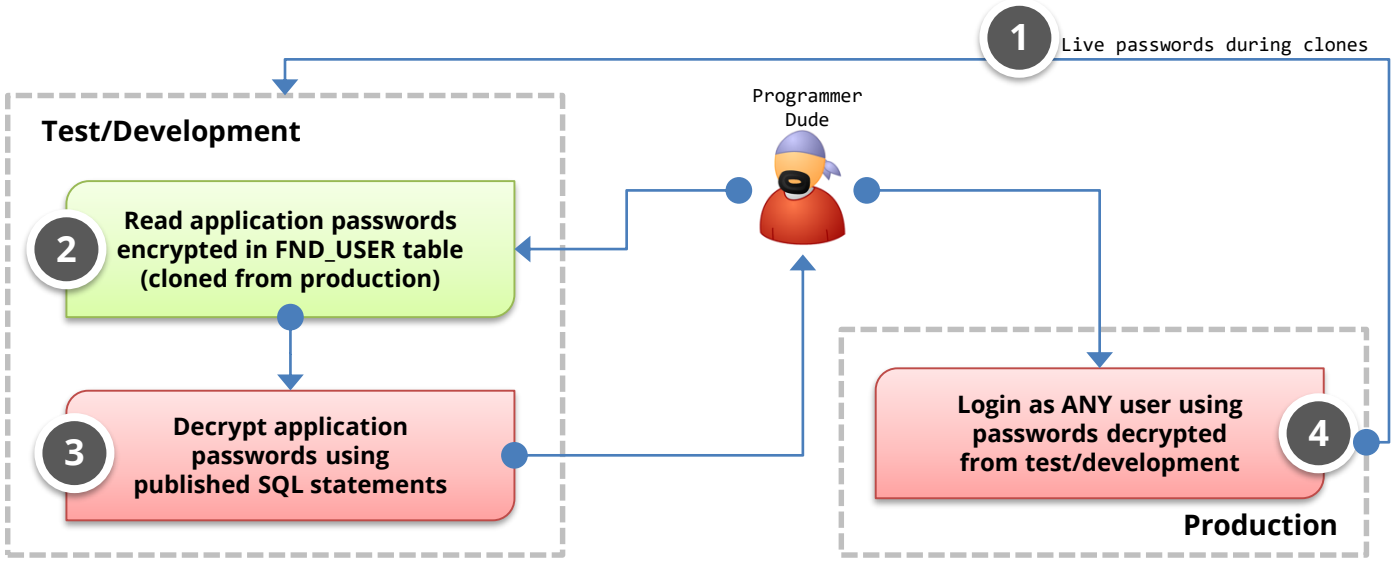
- **Apply Oracle Critical Patch Updates on a regular basis on all environments**
  - Reduce risk of compromise and escalation of privileges
  - Database PSU may be applied without EBS patch
  - Fusion Middleware/WebLogic patches often optional

- **Consider applying database, E-Business Suite, and application server patches independently**
  - Accelerate database patch if ad-hoc users
  - Accelerate E-Business Suite patch if DMZ
  - Review vulnerabilities in application server patches if DMZ

5

Threat

Application user passwords may be **decrypted** and multiple other user accounts may be used to circumvent application controls.



Oracle EBS Password Encryption

FND_USER Table

USER_NAME	ENCRYPTED_FOUNDATION_PASSWORD	ENCRYPTED_USER_PASSWORD
GUEST	ZG6EBD472D1208B0CDC78D7EC7730F9B249496F825E761BA3EB2FEBB54F6915FADA757EF4558CF438CF55D23FE32BE0BE52E	ZG6C08D49D524A1551A3068977328B1AFD260400FB598E799A3A8BAE573777E7EE7262D1730366E6709524C95EC6BFA0DA06
SYSADMIN	ZH39A396EDCA4CA7C8D5395D94D8C915510C0C90DA198EC9CDA15879E8B547B9CDA034575D289590968F1B6B38A1E654DD98	ZHF57EAF37B1936C56755B134DE7C83AE40CADDD4AA83B1D7455E5533DC041773B494D2AA04644FB5A514E5C5614F3C87888
WIZARD	ZG2744DCFCCFFA381B994D2C3F7ADACF68DF433BADF59CF6C3DAB3C35A11AAAB2674C2189DCA040C4C81D2CE41C2BB82BEC6	ZGE9AAA974FB46BC76674510456C739564546F2A0154DCF9EBF2AA49FBF58C759283C7E288CC673044036E284042A8EE4451

APPS password encrypted user name + user password

User password encrypted using APPS password

Oracle EBS Password Decryption

- **Application passwords by default are encrypted, not hashed which is more secure**
  - Default in all EBS versions including 12.2
  - Simple method to decrypt if able to access FND_USER table

- **Secure hashing of passwords is optional and must be enabled by DBA**
  - Patch for earlier 11i versions and included with R12 but not enabled by default

- **Encrypted application passwords are cloned to test and development databases**
  - See Integrigy whitepaper for recommendations

Password Decryption Recommendations

- **Be sure password hashing is enabled by DBAs**
  - DBAs must run FNDCPASS USERMIGRATE (MOS ID 457166.1)
  - Verify it has been run successfully for all users (MOS ID 1084956.1)

- **Change all application user passwords when cloning from production to test and development**
  - All environment credentials should be changed during clones
  - Enable forgot password functionality for accessing passwords

- **Enable strong application password controls in all Oracle EBS environments**
  - Prevents possible brute forcing of application password hashes

Oracle EBS Password Hash Feature

FND_USER Table

USER_NAME	ENCRYPTED_FOUNDATION_PASSWORD	ENCRYPTED_USER_PASSWORD
GUEST	XG{SHA1}	XG6C08D49D524A1551A3068977328B1AFD260400FB598E799A3A8BAE573777E7EE7262D1730366E6709524C95EC6BFA0DA06
SYSADMIN	XG{SHA1}	XGF57EAF37B1936C56755B134DE7C83AE40CADDD4AA83B1D7455E5533DC041773B494D2AA04644FB5A514E5C5614F3C87888
WIZARD	XG{SHA1}	XGE9AAA974FB46BC76674510456C739564546F2A0154DCF9EBF2AA49FBF58C759283C7E288CC673044036E284042A8FF4451

APPS password no longer encrypted and stored in FND_USER

User password now a SHA1 one-way hash

Hashed Password Hash Upgrade

For 12.1.3 and 12.2.3+, Oracle has upgraded the hashing algorithm to support SHA-256, SHA-384, and SHA-512. SHA-512 should always be used and also upgraded to if SHA1 hashing is already enabled. Upon password change, migrated to new hash algorithm if enabled.

12.1.3	▪ Apply 21276707:R12.FND.B ▪ First time, run AFPASSWD -m **SHA512** ▪ Already migrated, run AFPASSWD -m **SHA512 PARTIAL**
12.2.3+	▪ Apply 26175708 (FND.C) FND SECURITY RUP JUN-2017 (new hashes and many other FNDCPASS/AFPASSWD fixes) ▪ First time, run AFPASSWD -m **SHA512** ▪ Already migrated, run AFPASSWD -m **SHA512 PARTIAL**

Validate Hash Passwords Enabled SQL

Not all passwords may be migrated due to errors such as invalid characters in the username or password. Verify all passwords are migrated with the following query.

```
select *
from applsys.fnd_user
where encrypted_foundation_password not like 'X_{SHA%'
and encrypted_foundation_password not like 'VH%'
and encrypted_foundation_password != 'INVALID'
and encrypted_user_password != 'EXTERNAL';
```

6 Direct Database Access by Users

- **Database access is a key problem**
  - Look for accounts like APPS_RO, HR_READ, etc.
  - Read only accounts often created with read to all data
- **Access to sensitive data by generic accounts**
  - Granularity of database privileges (SELECT ANY TABLE vs. direct table grants)
  - Complexity of data model – 1,000's of tables
  - Number of tables/views and continuous development make it difficult to create limited privilege database accounts
  - Must use individual database accounts with roles limiting access to data along with other security

How to Review Direct Database Access

1. **Need to review who is accessing the database**
   - Must have auditing enabled to determine generic database access
   - **Oracle 12c Privilege Analysis feature now included with Enterprise Edition instead of with Database Vault**
2. **Difficult and time-consuming to review database privileges**
   - Must manually review database privileges
   - Need to understand data model, customizations, and interfaces to know what can be accessed and why with granted privileges

Integrigy #1 Security Recommendation

- **Limit direct database access whenever possible**
  - Much harder to hack database if attacker can not connect

- **Use firewalls in front of data center, network ACLs, TNS invited nodes, Oracle Connection Manager, Oracle Database Firewall, etc.**
  - DBAs should use bastion hosts to manage databases

7 SSL/TLS not configured

- **SSL/TLS encrypt network traffic between the end-user browser and the Oracle E-Business Suite web server**
  - When http:// is used, all traffic is sent across the network in clear text including passwords and sensitive data
- **SSL/TLS is not enabled by default in a E-Business Suite environment**
- **Recommended not to enable SSL/TLS on the E-Business Suite web server rather use the load balancer or reverse proxy as the SSL termination point**
  - Load balancer will have a more robust TLS stack and centralized administration of certificates

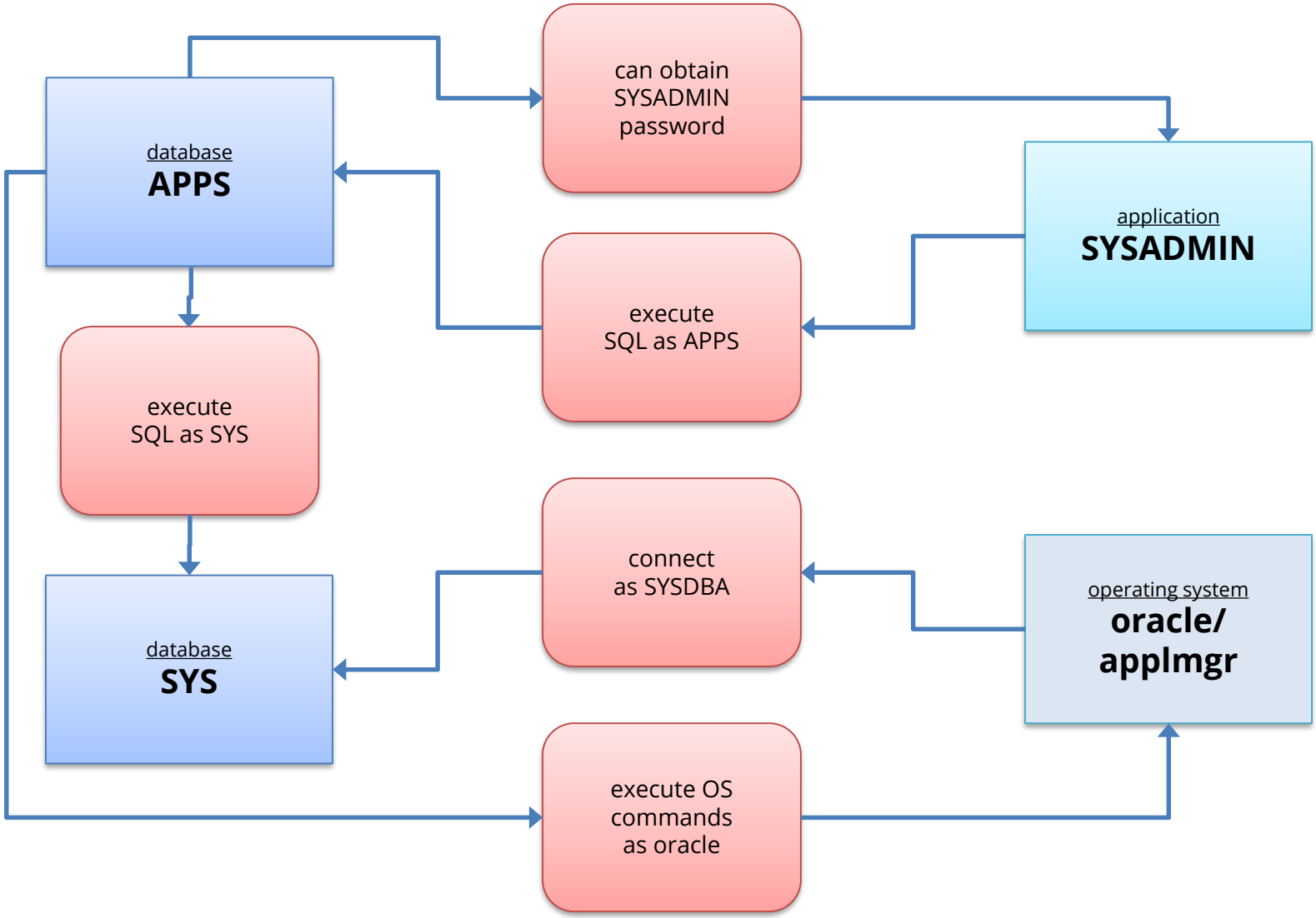
7 Enable SSL/TLS Internally and Externally

- **Oracle EBS TLS 1.2 certified**
  - Enabled in 12.1 (see 376700.1) and 12.2 (see 1367293.1)
  - Disable SSLv3, TLS 1.0, and TLS 1.1
- **Review the enabled ciphers and remove old or weak ciphers**
- **If deployed externally, use a site like ssllabs.com to verify the SSL/TLS configuration**

8 Oracle EBS Generic Privileged Accounts

Oracle E-Business Suite	**SYSADMIN** *seeded application accounts*
Oracle Database	**APPS, APPLSYS** **SYS, SYSTEM** *Oracle EBS schemas (GL, AP, ...)*
Operating System *(Unix and Linux)*	**root** **oracle, applmgr**

Generic Privileged Account Inter-Dependency



Best Practices for Controlling Privileged Accounts

- **Use a Bastion host (virtual desktop) for direct O/S and/or database access**
- **Consider Oracle Database Vault**
  - Additional license but comes with pack for E-Business Suite schemas
- **Periodically inventory privileged and generic accounts**
- **Adopt formal privileged account and password policy**
- **Use a password vault to store and control access to account passwords**
  - Unable to fully control in Oracle EBS but provides a layer of control

9 No Database or Application Auditing

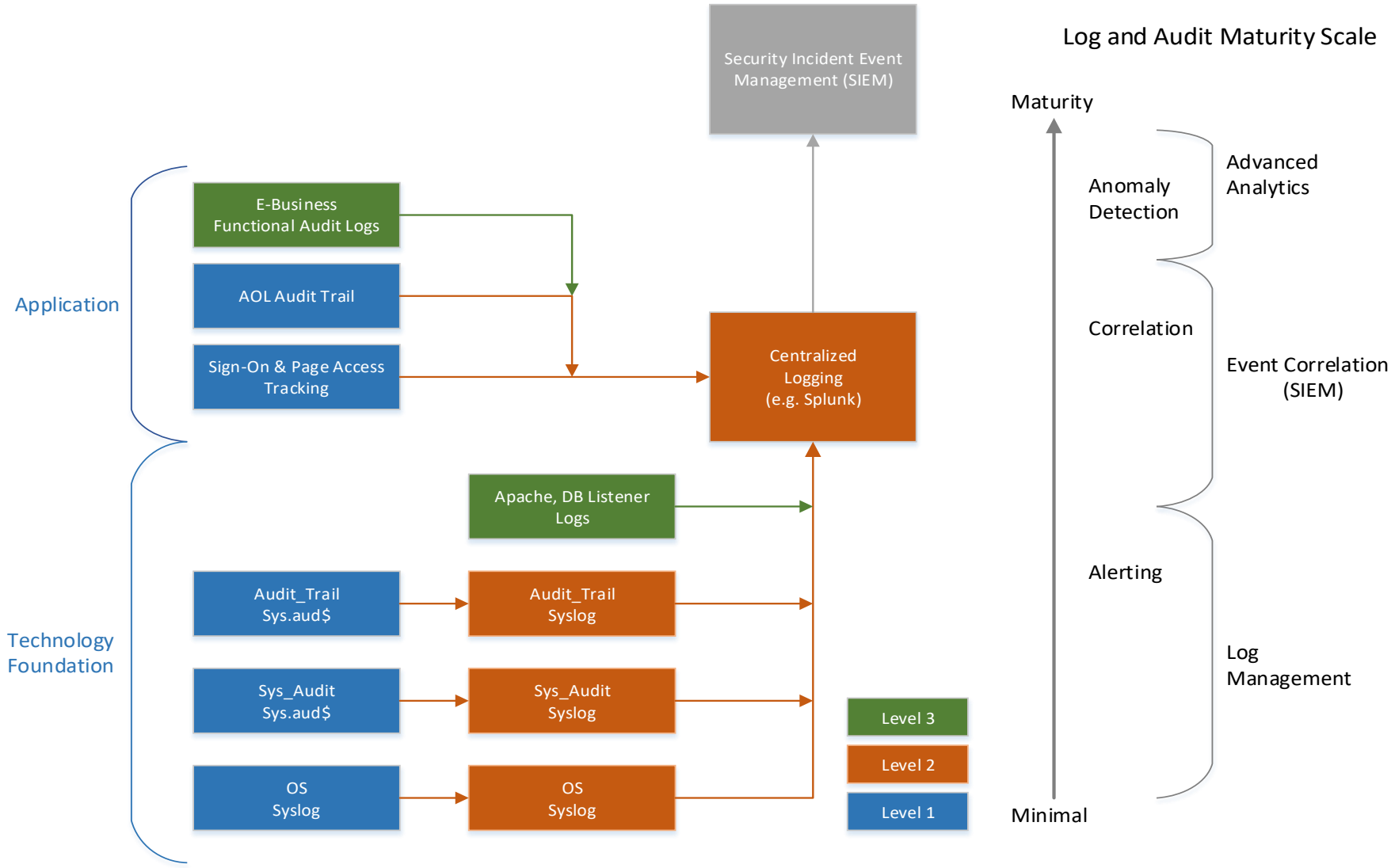
- **The Oracle database and Oracle E-Business Suite offer rich log and audit functionality**
  - **Most organizations do not fully take advantage**
- **Requirements are difficult**
  - Technical, Compliance, Audit, and Security
- **Integrigy has a framework**
  - Already mapped to PCI, HIPAA, SOX and 21 CFR 11

Logging and Auditing Is the Key

- **Access management success or failure largely based on logging and auditing**
  - No other way

- **Constantly log activity**
  - Focus on key events
  - Audit with reports
  - Alert in real-time

Oracle E-Business Suite Auditing



Sensitive data not encrypted at rest

- **Storage (Data at rest)**
  - **Disk, storage, media level encryption**
  - Encryption of data at rest such as when stored in files or on media
- **Access (Data in use)***
  - **Application or database level encryption**
  - Encryption of data with access permitted only to a subset of users in order to enforce segregation of duties
- **Network (Data in motion)**
  - **Encryption of data when transferred between two systems**
  - SQL*Net encryption (database)

Oracle Credit Card Encryption (no TDE)

- **Application-level encryption**
  - **Not enabled by default in 11i or R12**
  - Better solution than other technologies such as Oracle Transparent Data Encryption (TDE)
  - General patch release availability October 2006
  - Significant modification to application – 64 packages, 60 web pages, and 18 forms

- **11i = MOS Note ID 338756.1, Patch 4607647**
- **R12 = MOS Note ID 863053.1**
  - 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)

Misconceptions about Database Storage Encryption

- **Not an access control tool**
  - Encryption does not solve access control problems
  - Data is encrypted the same regardless of user
  - Coarse-grained file access control only
- **No malicious employee protection**
  - Encryption does not protect against malicious privileged employees and contractors
  - DBAs have full access
- **Key management determines success**
  - Access to Oracle wallets (TDE) controls everything
  - You and only you can should control the keys
- **More is not better**
  - Performance cost of encryption
  - Cannot encrypt everything

What does TDE do and not do?

- **TDE only encrypts "data at rest"**
- **TDE protects data if following is stolen or lost -**
  - disk drive
  - database file
  - backup tape of the database files
- **An authenticated database user sees no change**
- **Does TDE meet legal requirements for encryption?**
  - California SB1386, Payment Card Industry Data Security
  - Ask your legal department

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**