INTEGRIGY

New Oracle 12c Security Features
Oracle E-Business Suite Perspective

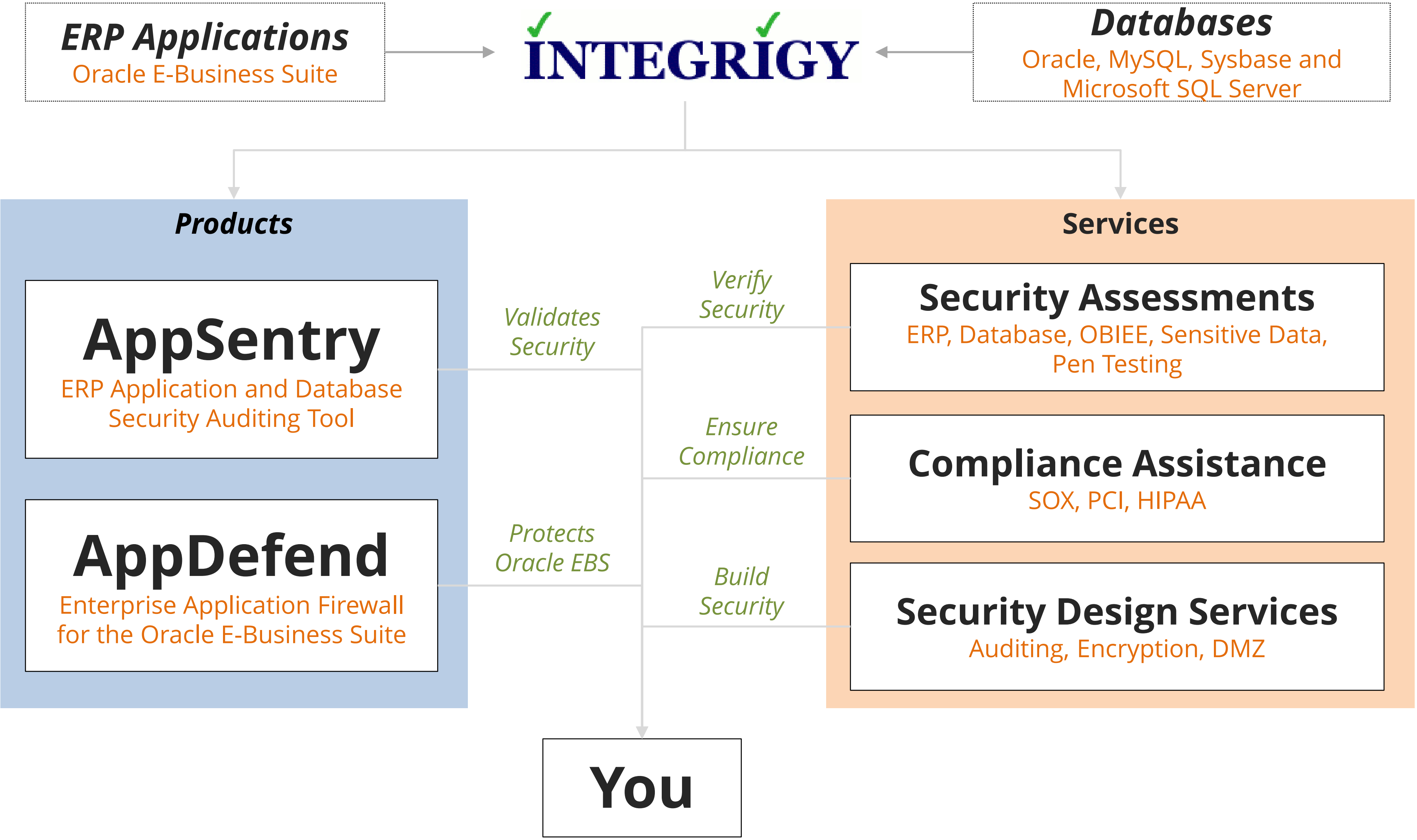
December 18, 2014

Michael Miller
Chief Security Officer
Integrigy Corporation

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, MySQL, Sysbase and Microsoft SQL Server

Products

AppSentry

ERP Application and Database Security Auditing Tool

AppDefend

Enterprise Application Firewall for the Oracle E-Business Suite

Services

Security Assessments

ERP, Database, OBIEE, Sensitive Data, Pen Testing

Compliance Assistance

SOX, PCI, HIPAA

Security Design Services

Auditing, Encryption, DMZ

Validates Security

Protects Oracle EBS

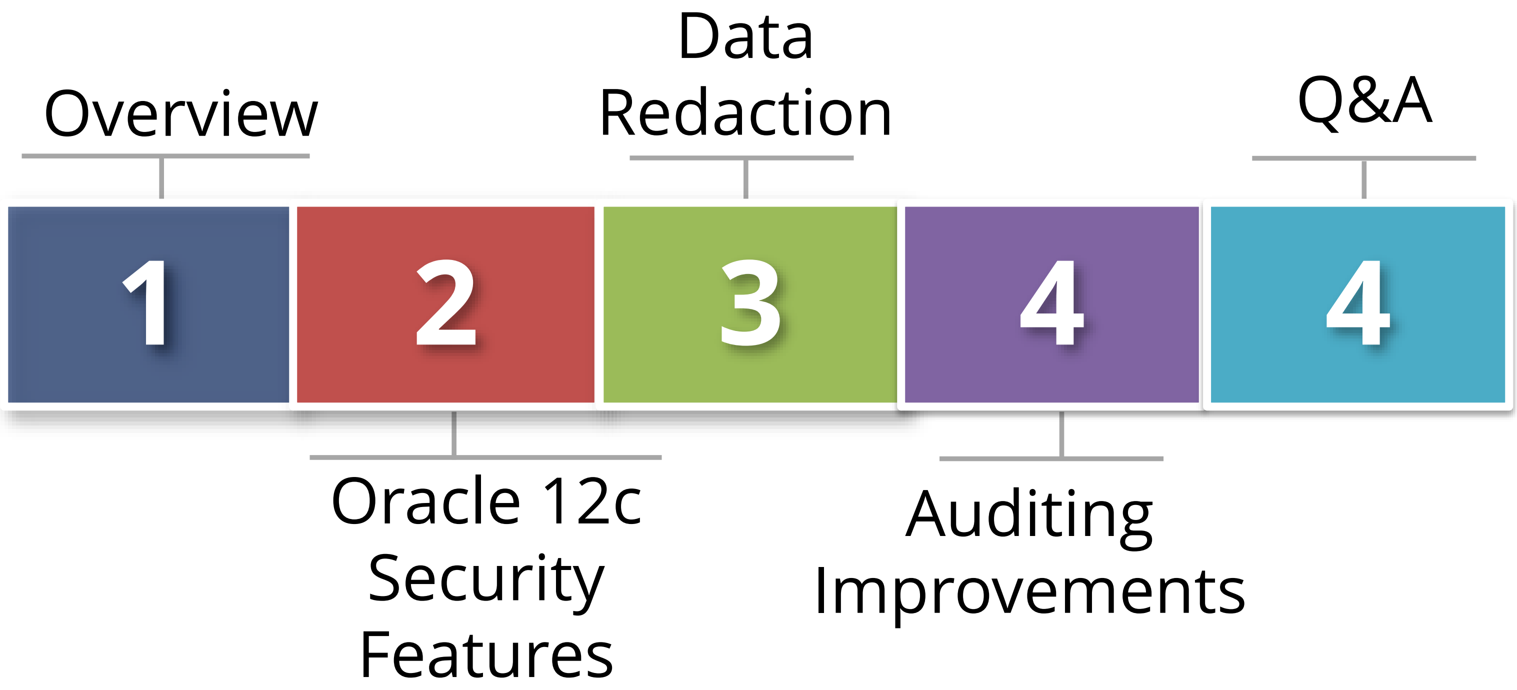
Verify Security

Ensure Compliance

Build Security

You

Agenda



1 Overview

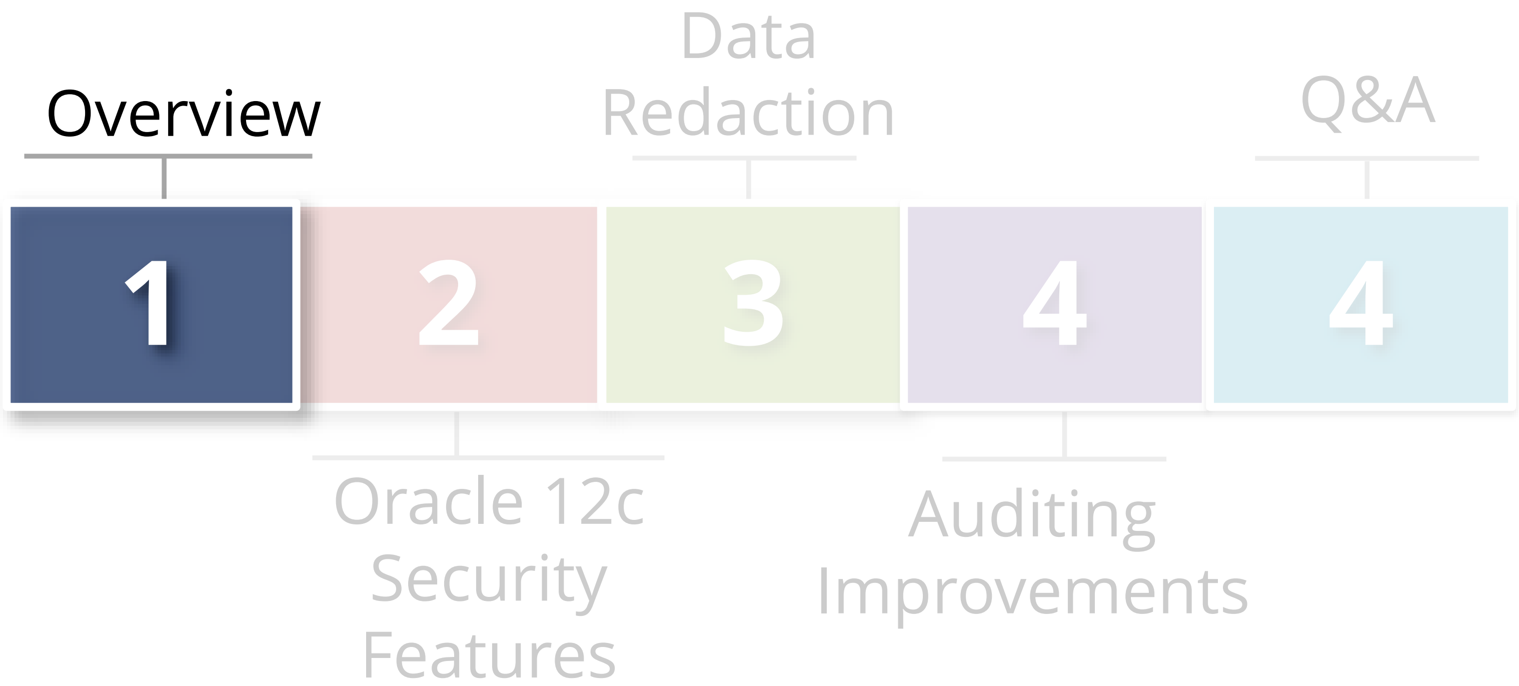
2 Oracle 12c Security Features

3 Data Redaction

4 Auditing Improvements

4 Q&A

Agenda



1 Overview

2 Oracle 12c Security Features

3 Data Redaction

4 Auditing Improvements

4 Q&A

Oracle 12c New Features

- **Major new features**
  - In-memory
  - Multitenant (pluggable databases)

- **Incremental security improvements**
  - Data Redaction
  - Real Application Security
  - Unified Auditing
  - Mandatory Auditing

Oracle 12c Now Certified For E-Business

- Oracle database release 12c as of 27-Sept-2014 is certified with the Oracle E-Business Suite release*
    - Oracle Multitenant not certified

*Source https://blogs.oracle.com/stevenChan/entry/12_1_0_2_db

Why Upgrade the Database?

- **Oracle E-Business Suite patches and upgrades do not maintain the supporting software**
  - Database needs to be patched separately

- **Oracle E-Business Suite requires using a certified version of the Oracle database**

- **New database features may be of value**

Premier, Extended and Sustaining Support

- **Premier** – General Availability (GA) date + 5 years.
- **Extended** – Security and bug fixes for additional support fee. Available for 3 years after end of Premier.
- **Sustaining** – Download only existing patches, no new patches, security or bug fixes. Is indefinite.

Database Release	GA Date	Premier Support End Date	Extended Support End Date
12.1	Jun 2013	Jul 2018	Jul 2021
11.2	Sep 2009	Jan 2015*	Jan 2018*
11.1	Aug 2007	Aug 2012	Aug 2015
10.2**	Jul 2005	Jul 2010	Jul 2013

*Extended Support fees have been waived for the period of Feb 2015 – Jan 2016
** 10g is on sustaining support, no exclusions

When Upgrading Don’t Forget Security Patches

- **Database upgrades only contain the CPU patches available at the time of their release**
  - Your upgrade date will be later
  - Always apply the latest security (CPU) patch

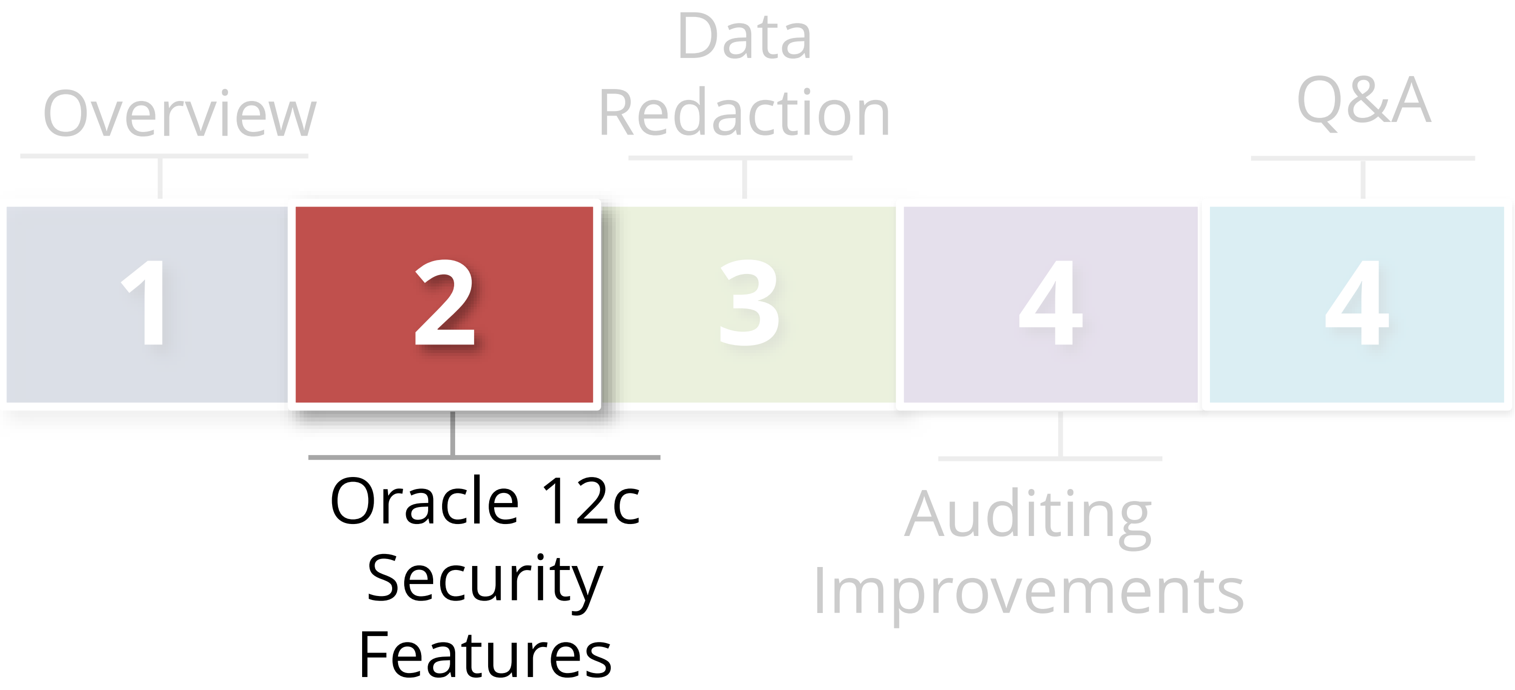
Upgrading Oracle E-Business Suite to Oracle 12c

- Follow Oracle Support Note ID 1524398.1 "Interoperability Notes EBS 12.0 or 12.1 with RDBMS 12cR1"

- **Integrigy recommendations:**
  - **Step 8** – Apply the latest CPU.
  - **Step 11** – Oracle Database Vault must be disabled when upgrading. Ensure to re-enable and that IT Security is aware.
  - **Step 15** – Drop the DMSYS schema. No longer used.
  - **Step 16 -** Review security related initialization parameters per security best practices.
  - **Step 20** - For Oracle E-Business Suite 12.1, the sqlnet_ifile.ora requires new initialization parameters.

*More information in blog post: http://www.integrigy.com/oracle-security-blog/oracle-e-business-suite-database-12c-upgrade-security-notes

Agenda



Overview

Data Redaction

Q&A

1

2

3

4

4

Oracle 12c Security Features

Auditing Improvements

New Oracle 12c Standard Components

- **Oracle Database Vault (DV) pre-installed**
  - Secure privileged user access
  - Privilege analysis reporting
  - Pre-built realms for E-Business Suite
  - Need additional license to use

- **APEX now mandatory**
  - APEX provided with standard database license
  - APEX/XML DB cannot be uninstalled
  - APEX integration and/or extensions with E-Business can be easily done but must be secured
  - Disable embed APEX listener if not using

Real Application Security

- **New with Oracle 12c**
  - Next generation VPD
  - Ideal for APEX applications
- **Define users separately from DBA_USERS**
  - DBA_XS_USERS
  - Can directly connect to the database
  - Flag in 12.1.0.2
- **Log RAS users using Unified Audit Trail**
  - XS$NULL vs. xs_user_name
- **RAS role and event auditing with Unified Audit**

New Oracle 12c Password Protection

- Password file now can be stored in ASM
  - If running RAC, now need only one password file
- Passwords by default are case sensitive
- New password verify functions
- Stronger password hash

Improved Separation of Duties

- **SYSDBA system privilege now segregated. SYSDBA still exists, but new privileges added**
  - SYSBACKUP for rman
  - SYSDG for Data Guard
  - SYSKM for managing TDE (encryption) keys

- **Benefits**
  - Junior DBAs no longer need highly privileged account to manage backups
  - Key management can now be delegated to staff other than DBAs

New Oracle 12c Protection for SYS User

- No brute-force lock-out protection until now

- Oracle 12c delivers a new hidden parameter '_sys_logon_delay'
  - Protects all Oracle 12c password file users such as SYS, SYSKM, SYSDG and SYSBACKUP

To query the parameter use this SQL:

```
SELECT A.KSPPINM "PARAMETER",
       B.KSPPSTVL "SESSION VALUE",
       C.KSPPSTVL "INSTANCE VALUE"
FROM   X$KSPPI A,
       X$KSPPCV B,
       X$KSPPSV C
WHERE  A.INDX = B.INDX
AND    A.INDX = C.INDX
AND    A.KSPPINM  = '_sys_logon_delay';
```

For more information refer to:

How To Query And Change The Oracle Hidden Parameters In Oracle 10g,11g and 12c (Doc ID 315631.1)

New READ Privileges

- **READ Object**
  - READ object privilege enables users to query, but not modify database tables, views, materialized views and synonyms
  - SELECT object privilege can still be used
  - SELECT object privilege also allows users to lock rows when reading

- **READ ANY TABLE**
  - Allows user to query any table in the database
  - GRANT ALL PRIVILEGES TO user SQL also now includes the READ ANY TABLE system privilege as well as the READ object privilege

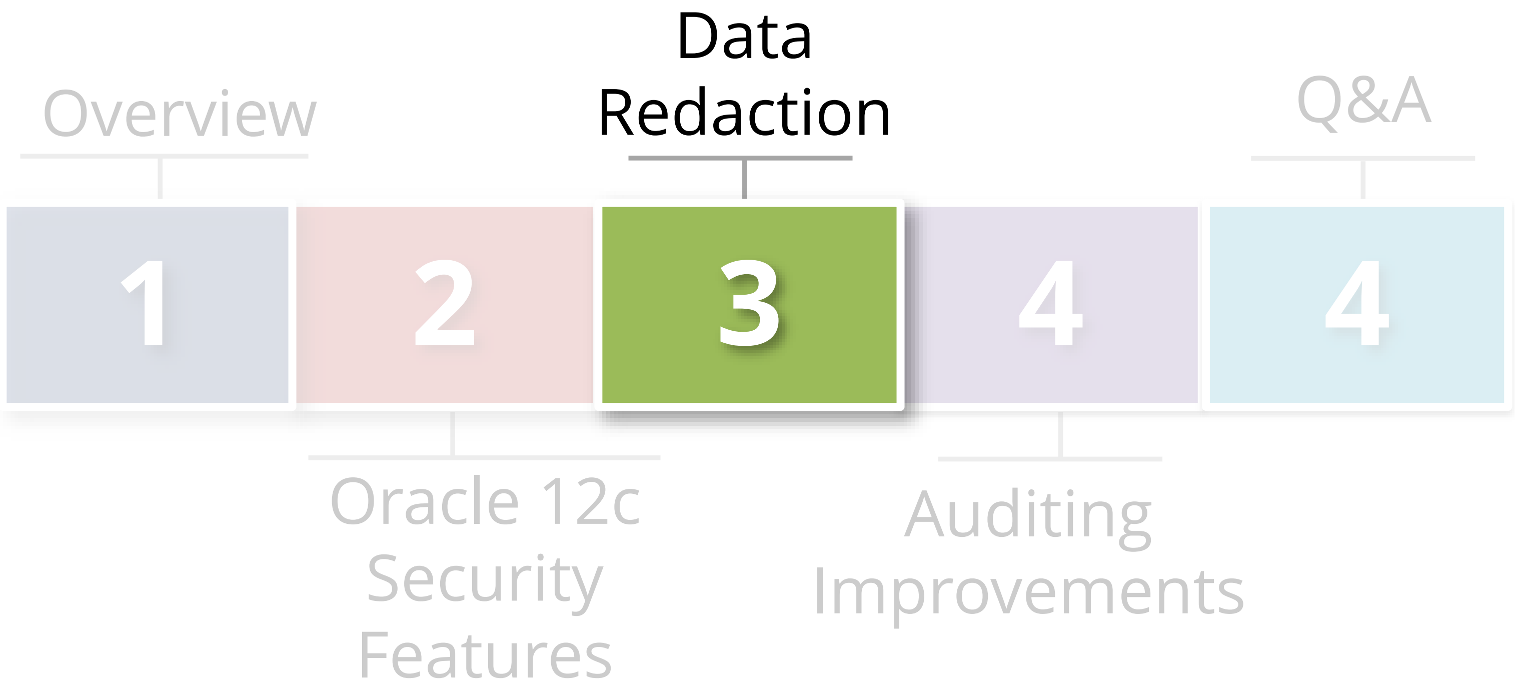
Oracle 12c Improvements to TSDP

- Transparent Sensitive Data Protection (TSDP)
  - New functionality, views and Cloud Control integration

- Use TSDP to identify, create and manage policies to protect sensitive data. Use with -
  - Oracle Data Redaction, Oracle Virtual Private Database, unified auditing, fine-grained auditing, and Transparent Data Encryption

- Oracle Application Accelerator for E-Business Suite
  - Lists and locates sensitive data (standard)
  - Facilitates masking and can use with OEM/TSDP
  - Additional license cost

Agenda



1 Overview

2 Oracle 12c Security Features

3 Data Redaction

4 Auditing Improvements

4 Q&A

Data Masking vs. Data Redaction

- **Data Masking**
  - Data is altered “obfuscated”
    - SSN of 111-11-1111 updated to 888-22-9999
  - Use to protect non-production data
  - Oracle Enterprise Manager Masking Pack
  - E-Business Suite Application Accelerator (masking)

- **Data Redaction**
  - Data is not altered
    - SSN of 111-11-1111 displayed as XXX-XX-1111
  - Use with non-production or production data
  - Oracle Data Redaction/Advanced Security Option

Oracle Data Redaction

- **What does Oracle Data Reaction do?**
  - Prevents unauthorized users from viewing sensitive data
  - Provides selective, on-the-fly redaction of sensitive data prior to display
  - Assists with compliance for Payment Card Industry data Security Standard (PCI DSS) and the Sarbanes-Oxley Act
- **How does it work?**
  - Policies defined to redact “mask” sensitive data by table/column
  - Redaction policies applied at runtime (at query-execution time)
  - No impact to data processing, replication, backup or import/export
- **Provided through Advanced Security Option (ASO)**
  - Installed by default, need additional license to use
  - Oracle 12c ASO is certified with E-Business Suite*

*Source https://blogs.oracle.com/stevenChan/entry/12_1_0_2_db

Data Redaction Methods

- **Full Redaction** - For example, SSN displayed as XXX-XX-XXXX.
- **Partial Redaction** - For example, SSN displayed as XXX-XX-1234.
- **Random Redaction** - Redacted data randomly generated values each time is displayed. For example, SSN 555-55-5555 and 777-77-7777
- **Regular Expressions** – Use regular expressions to look for patterns of data to redact.
- **No Redaction** – Used for testing redaction policies.

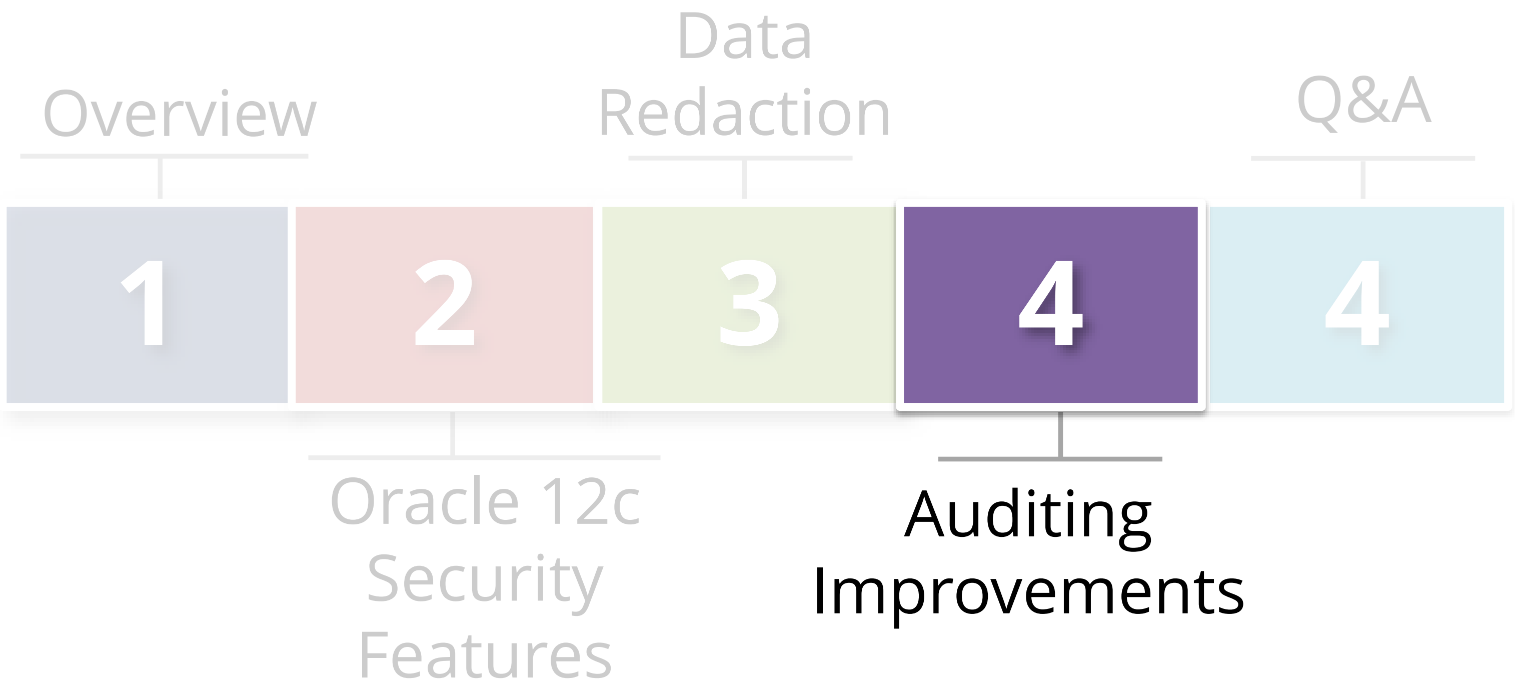
Data Redaction General Usage Guidelines

- Is NOT enforced for users using the **SYSDBA** administrative privilege
- Not intended to protect against attacks by regular and privileged database users who run ad-hoc queries directly against the database
- Not intended to protect against ad-hoc SQL queries that attempt to determine the actual values by inference
- DDL SQL that copies actual data (e.g. CREATE TABLE AS SELECT, INSERT AS SELECT) is blocked unless user granted EXEMPT_REDACTION_POLICY privilege
- Cannot use redacted columns in GROUP By clauses

Oracle E-Business Suite and Data Redaction

Use Data Redaction For	Do Not Use Data Redaction For
Reporting outside E-Business Suite.	Within the E-Business Suite.
Protecting sensitive data in direct connections to the E-Business Suite or data warehouse using reporting tools (such as OBIEE or BI Publisher).	Protecting DBAs, SYSDBA and privileged database users (or anyone with APPS password) from accessing sensitive data.
Protection of sensitive data in production databases.	Redacting non-production data. Is possible but recommend Masking "scrambling" non-production sensitive data.
Complementing or strengthening security provided by Unified Audit, TDE, TSDP, FGA, FGAC and VPD solutions.	Protecting sensitive data in ad-hoc queries.

Agenda



1

Overview

2

Oracle 12c Security Features

3

Data Redaction

4

Auditing Improvements

4

Q&A

Oracle 12c Mandatory Auditing

- New Oracle 12c **always-on-auditing** for SYSDBA
  - SYS, SYSDBA, SYSOPER, SYSASM, SYSBACKUP,
  - SYSDG, SYSKM

- Mandatory Auditing Events (can be found in (SYS.UNIFIED_AUDIT_TRIAL)
  - CREATE AUDIT POLICY
  - ALTER AUDIT POLICY
  - DROP AUDIT POLICY
  - AUDIT
  - NOAUDIT
  - Database Vault configurations
  - DBMS_FGA PL/SQL package
  - DBMS_AUDIT_MGMT PL/SQL package
  - ALTER TABLE attempts on the AUDSYS audit trail

Last Login Date

- Knowing when users last logged-in is required for effective user account management and auditing
- New with Oracle 12c is **Last_login** date added to **sys.dba_users**

```
SELECT USERNAME, ACCOUNT_STATUS, COMMON, LAST_LOGIN
FROM SYS.DBA_USERS
ORDER BY LAST_LOGIN ASC;
```

Username	Account Status	Common	Last Login
C##INTEGRIGY	OPEN	YES	05-AUG-14 12.46.52.000000000 PM AMERICA/NEW_YORK
C##INTEGRIGY_TEST_2	OPEN	YES	02-SEP-14 12.29.04.000000000 PM AMERICA/NEW_YORK
XS$NULL	EXPIRED & LOCKED	YES	02-SEP-14 12.35.56.000000000 PM AMERICA/NEW_YORK
SYSTEM	OPEN	YES	04-SEP-14 05.03.53.000000000 PM AMERICA/NEW_YORK

Two New Auditing Roles

- To better improve segregation of duties, Oracle 12c delivers two new database roles to use with auditing:
  - **AUDIT_ADMIN** - audit configuration and audit trail administration
  - **AUDIT_VIEWER** - viewing and analyzing audit data

New Way to Audit Databases – Unified Auditing

- **New features and syntax**

- **Two modes**
  - Pure Mode
  - Mixed (Default) Mode

Unified Auditing Mixed Mode

- **All traditional audit features and functionality work same as before**
  - Default Oracle 12c
  - Provided as a transition

- **Unified Audit Trail populated in parallel to traditional auditing**
  - Because default policy ORA_SECURECONFIG
  - Purge or disable ORA_SECURECONFIG Doc ID 1624051.1

Unified Auditing Pure Mode

- **Not default, but is the future**
  - Implemented in SGA for increased performance
  - Re-link kernel to use
- **Traditional auditing not populated**
- **Has new parameters and syntax**
  - Old init.ora parameters ignored
- **Uses OracleSecure files**
  - No syslog
- **Can revert back to Mixed Mode**

New Audit Feature: Audit Any Role

- **Any database role can be audited, including user-created roles**
  - Audits all system privileges granted to a role
  - Eliminates need to update audit policies when roles are updated
  - Unified Audit functionality available in both Mixed and Pure mode

```
CREATE AUDIT POLICY role_dba_audit_pol
ROLES DBA
CONTAINER = ALL;
AUDIT POLICY role_dba_audit_pol;
```

The Unified Auditing Super View

Works the same in either Mixed Mode or Pure Mode

SYS.UNIFIED_AUDIT_TRAIL Content*	**Number of Columns**
Standard auditing including SYS audit records	44
Real Application Security (RAS) and RAS auditing	17
Oracle Label Security	14
Oracle Data Pump	2
Fine grained audit (FGA)	1
Data Vault (DV)	10
Oracle RMAN	5
SQL*Loader Direct Load	1
Total	94

*Key column is AUDIT_TYPE

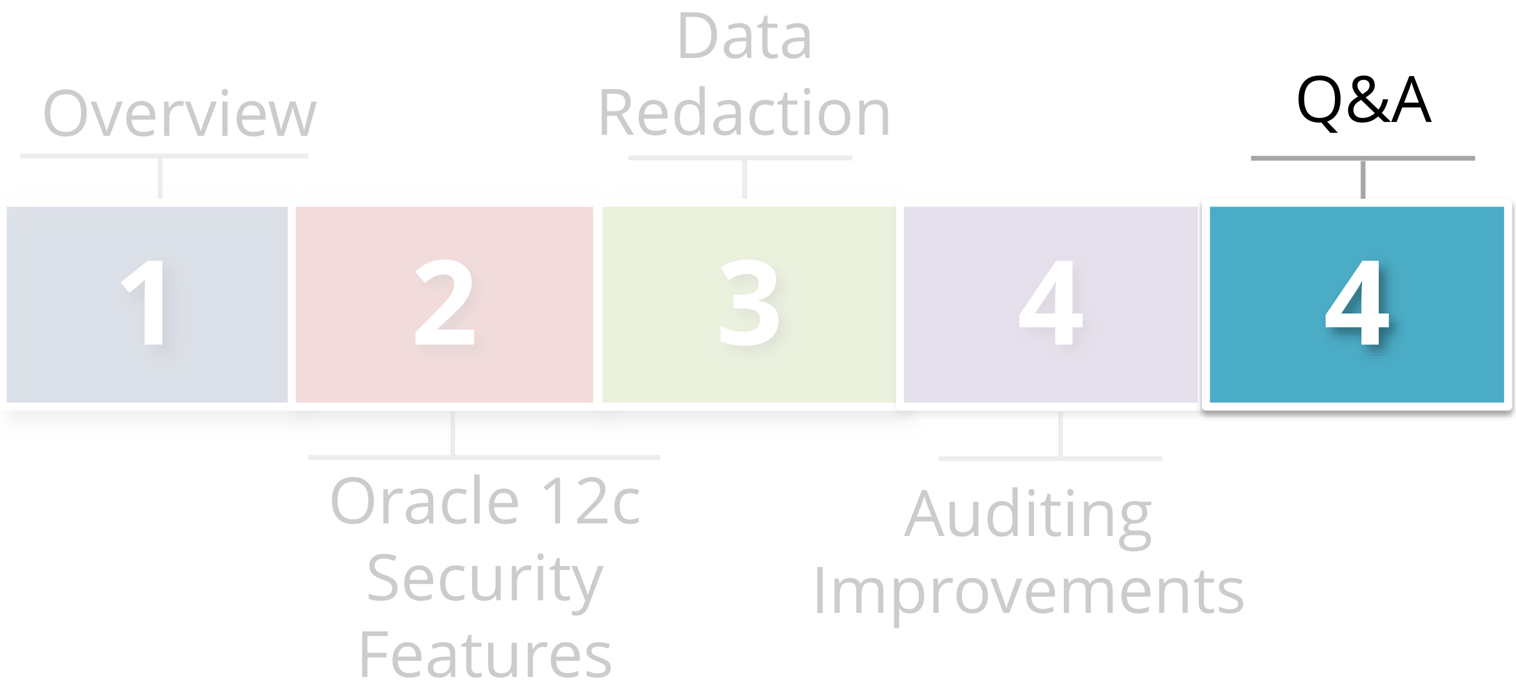
Oracle E-Business Suite and Unified Auditing

- Use Mixed Mode (12c Default)
- For new audit requirements consider Unified Audit polices and features
- Use SYS.UNIFIED_AUDIT_TRAIL for reporting
- Remember to disable policy or purge activity for ORA_SECURECONFIG

Oracle Client Identifier

Application	Example of how used
E-Business Suite	As of Release 12, the Oracle E-Business Suite automatically sets and updates CLIENT_IDENTIFIER to the FND_USER.USERNAME of the user logged on. Prior to Release 12, follow Support Note How to add DBMS_SESSION.SET_IDENTIFIER(FND_GLOBAL.USER_NAME) to FND_GLOBAL.APPS_INITIALIZE procedure (Doc ID 1130254.1)
PeopleSoft	Starting with PeopleTools 8.50, the PSOPRID is now additionally set in the Oracle database CLIENT_IDENTIFIER attribute.
SAP	With SAP version 7.10 above, the SAP user name is stored in the CLIENT_IDENTIFIER.
Oracle Business Intelligence Enterprise Edition(OBIEE)	When querying an Oracle database using OBIEE the connection pool username is passed to the database. To also pass the middle-tier username, set the user identifier on the session. Edit the RPD connection pool settings and create a new connection script to run at connect time. Add the following line to the connect script: CALL DBMS_SESSION.SET_IDENTIFIER('VALUEOF(NQ_SESSION.USER)')

Agenda



1 Overview

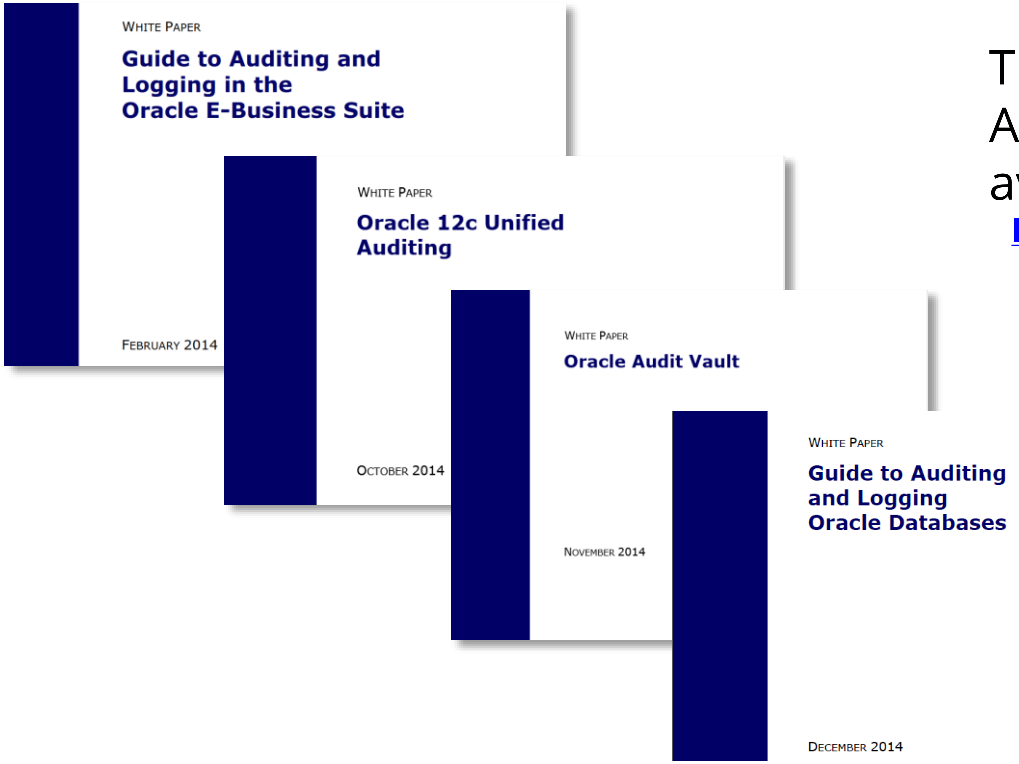
2 Oracle 12c Security Features

3 Data Redaction

4 Auditing Improvements

4 Q&A

Integrigy Oracle Whitepapers



WHITE PAPER

Guide to Auditing and Logging in the Oracle E-Business Suite

FEBRUARY 2014

WHITE PAPER

Oracle 12c Unified Auditing

OCTOBER 2014

WHITE PAPER

Oracle Audit Vault

NOVEMBER 2014

WHITE PAPER

Guide to Auditing and Logging Oracle Databases

DECEMBER 2014

This presentation is based on our Auditing and Logging whitepapers available for download at –

http://www.integrigy.com/security-resources

Contact Information

Michael Miller

Chief Security Officer

web: **www.integrigy.com**

e-mail: **info@integrigy.com**

blog: **integrigy.com/oracle-security-blog**

youtube: **youtube.com/integrigy**