The Thrifty DBA™ Does
Database Security

May 11, 2017

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

About Integrigy

ERP Applications
Oracle E-Business Suite,
PeopleSoft, Oracle Retail

INTEGRIGY

Databases
Oracle, Microsoft SQL Server,
DB2, Sybase, MySQL

Products

AppSentry
ERP Application and Database
Security Auditing Tool

Validates Security

AppDefend
Enterprise Application Firewall
for the Oracle E-Business Suite
and Oracle PeopleSoft

Protects Oracle EBS & PeopleSoft

Services

Verify Security

Security Assessments
ERP, Database, Sensitive Data, Pen Testing

Ensure Compliance

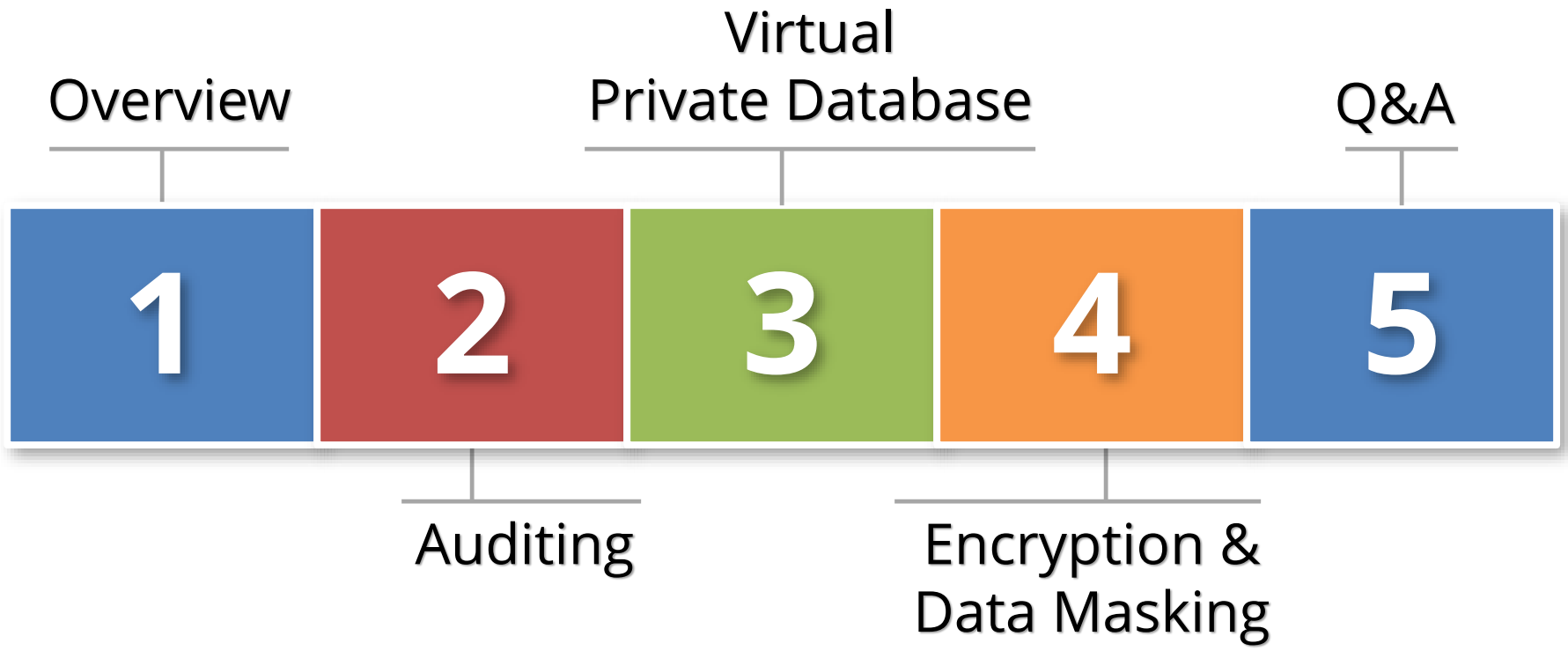
Compliance Assistance
SOX, PCI, HIPAA, GLBA

Build Security

Security Design Services
Auditing, Encryption, DMZ

Integrigy Research Team
ERP Application and Database Security Research

Agenda


Overview
Virtual
Private Database
Q&A
1
2
3
4
5
Auditing
Encryption &
Data Masking

thrift·y [**thrif**-tee]

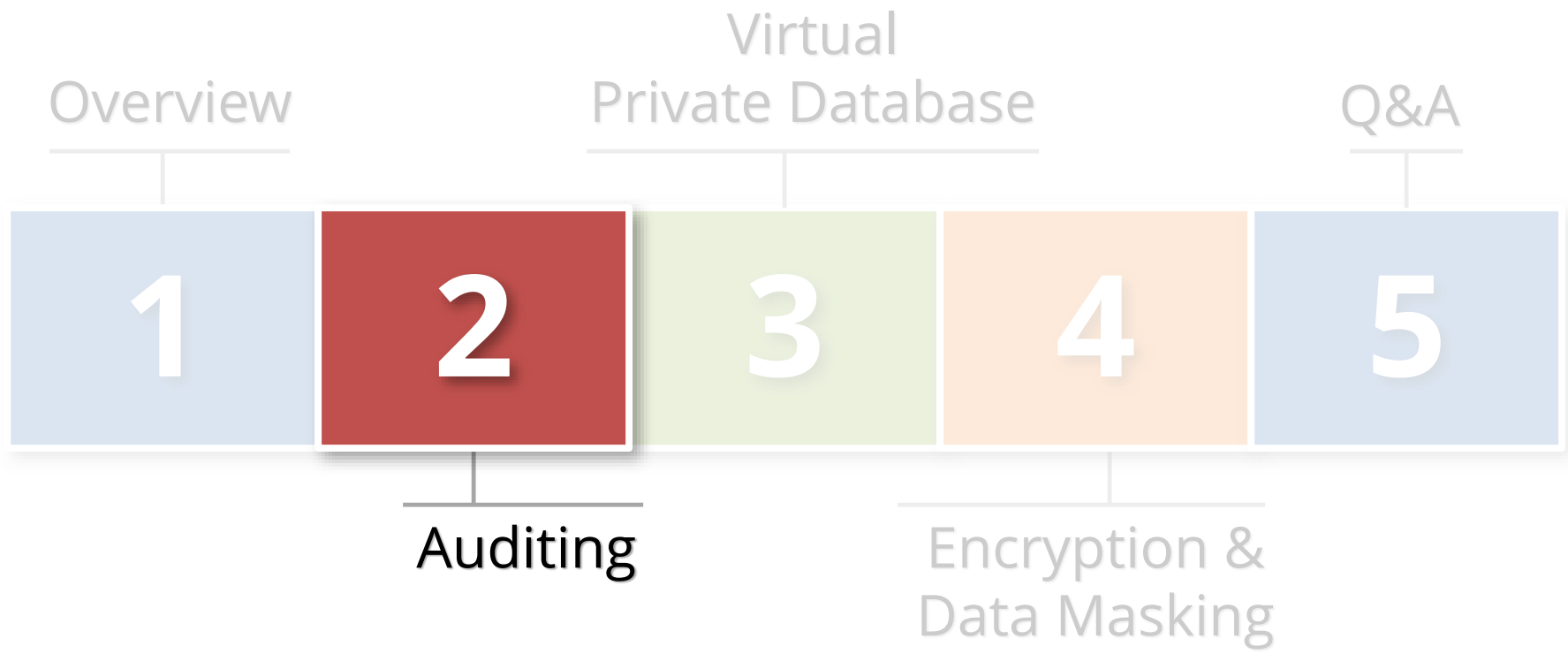
adjective

1. using money or other resources carefully and wastefully.
2. thriving, prosperous, or successful.
3. saving money by not buying unnecessary security products.

Oracle Database Editions – Security Features

	Express 11g	Standard	Enterprise
Transparent Data Encryption (TDE)			Option
Real Application Security			✓
Database Vault			Option
Data Masking			Option
Redaction			Option
Label Security			Option
Secure Application Roles			Option
Virtual Private Database (VPD)			✓
Fine-Grained Auditing (FGA)			✓
Proxy Authentication		✓	✓
Data Encryption Toolkit	✓	✓	✓

Agenda


Overview
Virtual Private Database
Q&A
1
2
3
4
5
Auditing
Encryption & Data Masking

Auditing Security Requirements

- Must audit key database security events and access by generic accounts
- Audit trail must be retained and protected centrally
- Alerts for potential security incidents must be raised
- Audit trail must be archived for forensic purposes
- May require auditing of access to key application tables that contain sensitive data

Commercial Auditing Solutions

There are a number of commercial database activity monitoring (DAM) solutions available at significant cost and implementation effort.

Oracle Audit Vault	▪ Licensing per processor monitored or audited ▪ $ 6,000 per processor license ▪ $ 1,320 per processor support and maintenance
Imperva	▪ Starting at $ 40,000 for 25 databases ▪ Starting at $ 6,400 per year support and maintenance
IBM Guardium	▪ Starting at about $ 60,000 including first year support and maintenance

Pricing is from the Oracle Technology Global Price List (12/16) and other sources. Actual cost will vary based on implementation, number of databases, and discounts.

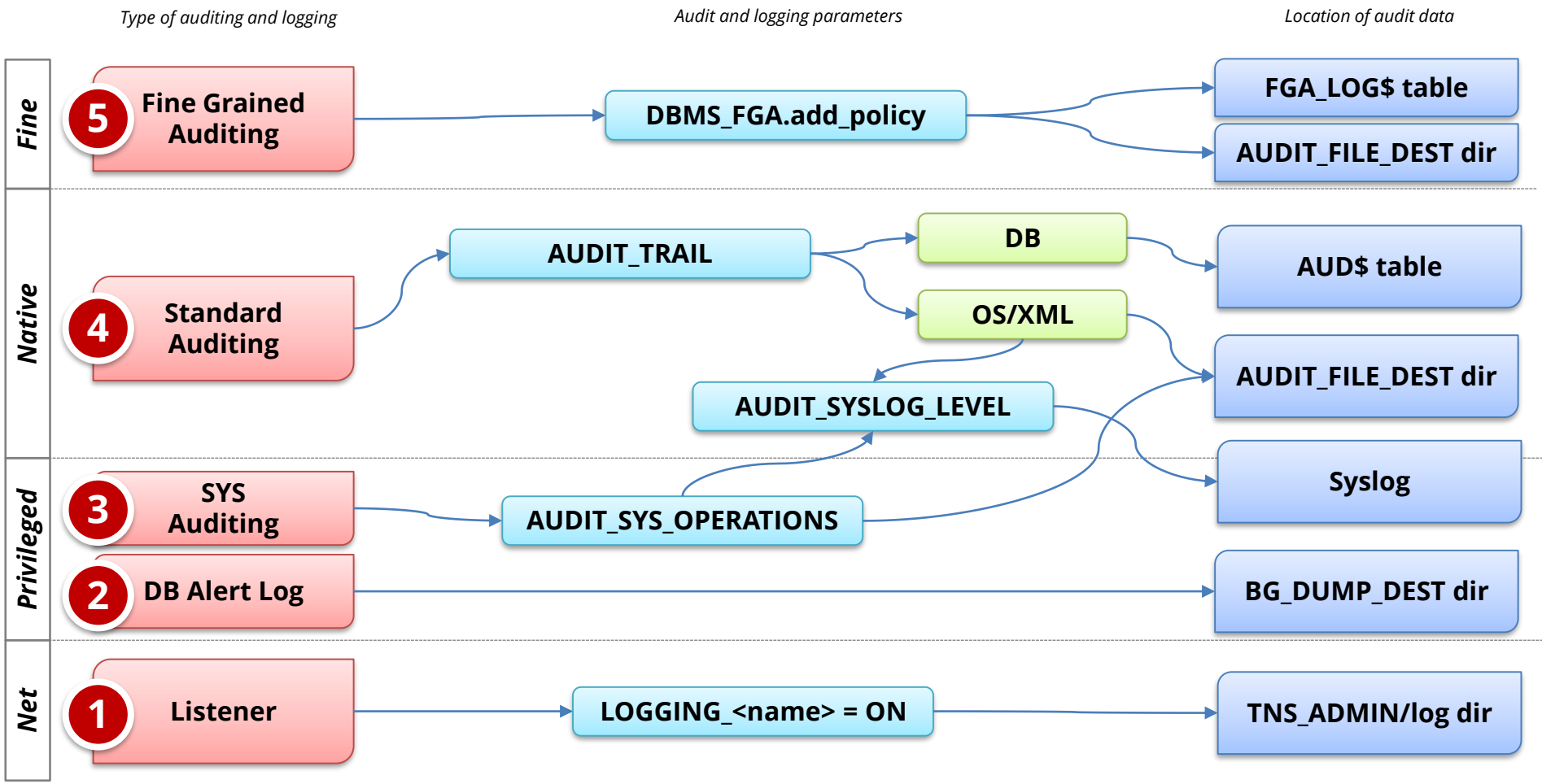
Auditing Design

Use Integrigy Database Auditing and Logging Framework as starting point!

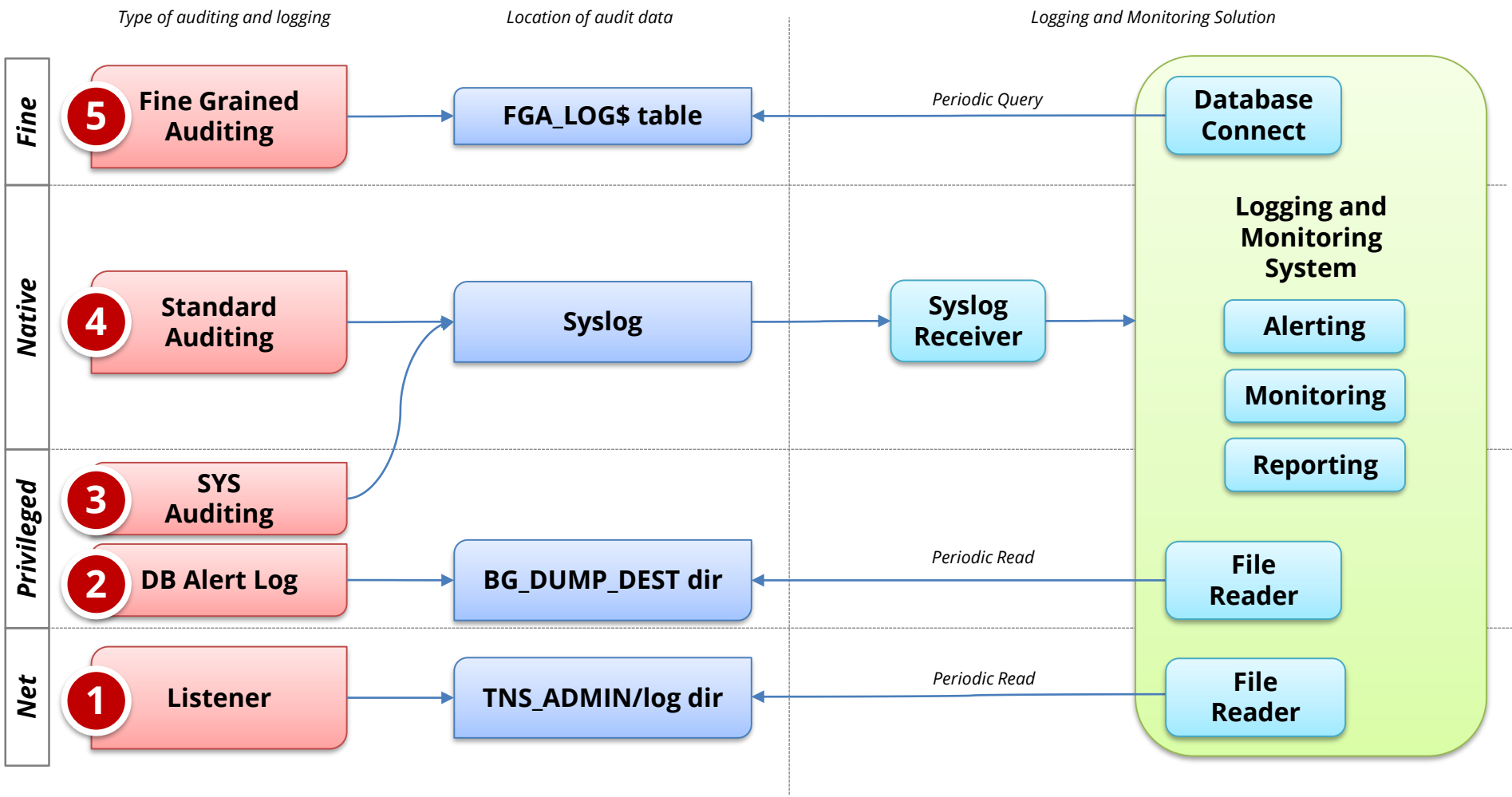
E1 - **Login**	*E8* - **Modify role**
E2 - **Logoff**	*E9* - **Grant/revoke user privileges**
E3 - **Unsuccessful login**	*E10* - **Grant/revoke role privileges**
E4 - **Modify auth mechanisms**	*E11* - **Privileged commands**
E5 - **Create user account**	*E12* - **Modify audit and logging**
E6 - **Modify user account**	*E13* - **Create, modify or delete object**
E7 - **Create role**	*E14* - **Modify configuration settings**

https://www.integrigy.com/security-resources/integrigy-guide-database-auditing-and-logging

Traditional Database Auditing (pre 12c, 12c Mixed Mode)



Traditional Database Auditing (pre 12c, 12c Mixed Mode)



Centralized Logging Solutions (Free, On-premise)

Splunk Free	▪ 500MB/day ▪ No signon security ▪ Splunk DB Connect add-on ▪ Splunk Oracle Database add-on
ELK (Elastic Search, Logstash, Kibana, Beats)	▪ Open Source ▪ Visualizations using Kibana ▪ Add-ons for alerting and reporting
GrayLog	▪ Open Source ▪ Based on Elastic Search and MongoDB ▪ Alerting, dashboards, and searching

Database Audit Trail – SYSLOG

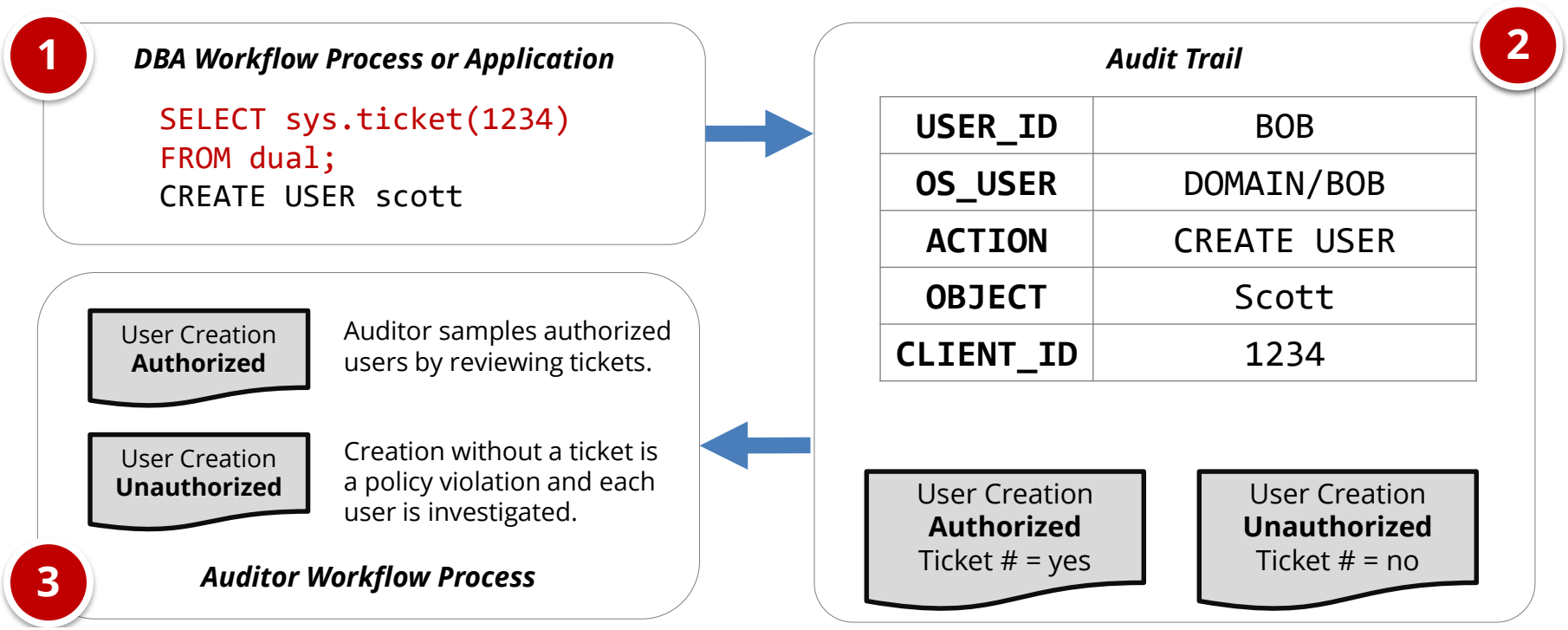
- **AUDIT_SYSLOG_LEVEL = facility.priority**
  - Available starting with 10.2
  - Set AUDIT_TRAIL=OS
  - Audit trail and SYS audit trail written to standard Unix/Linux Syslog
  - Can only be modified by root and completely protected from DBA, except disabling auditing
  - Send to external logging system using standard Syslog functionality (@<ip address>)

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)')

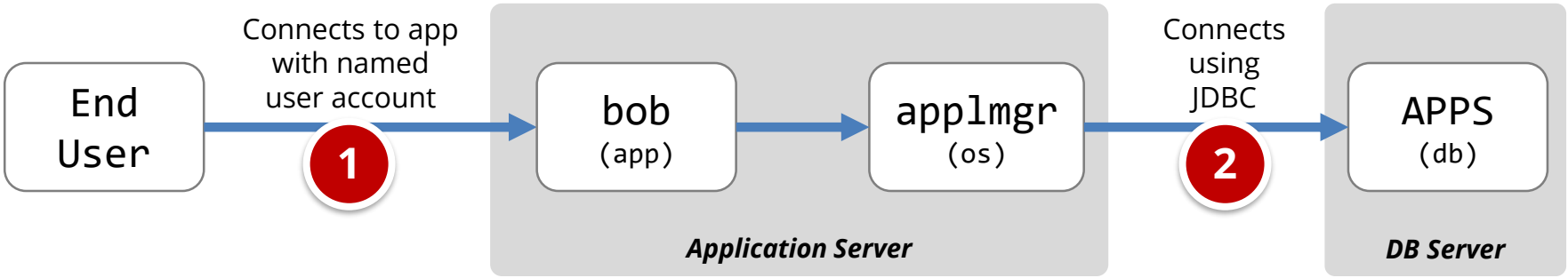
Change Ticket Tracking – Create User Example

Capture ticket numbers and other information for a database session based on special SQL executed by database users or applications.



Application End User Tracking – Solution

Capture web application end-users and correlate the application end-user to SQL statements. Support depends on the application or change to application code.

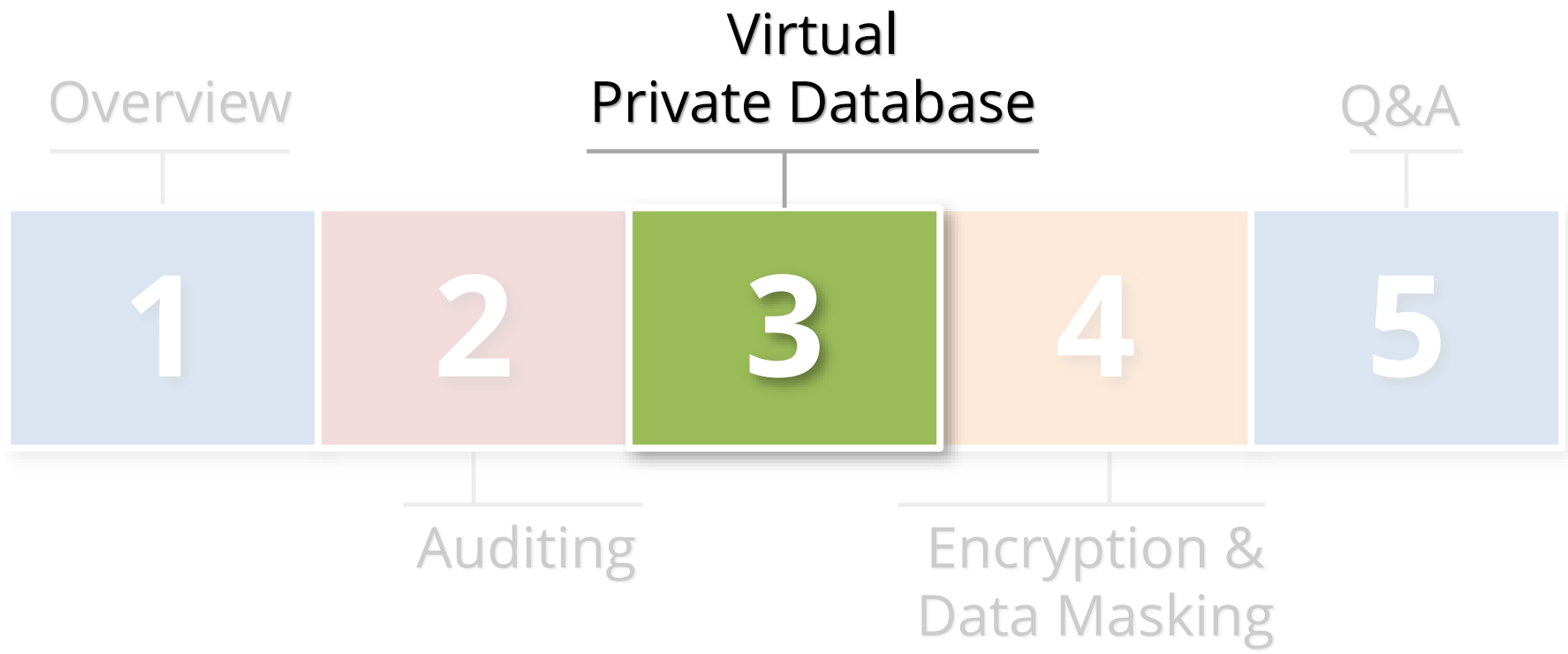


Solution Audit Record with "Application User" Feature Enabled

DB User	OS User	Machine	SQL	Client Identifier
APPS	applmgr	APPSERVER1	select * from credit_cards	bob

This example is Oracle E-Business Suite R12

Agenda


Overview
Virtual
Private Database
Q&A
1
2
3
4
5
Auditing
Encryption &
Data Masking

Data Access Security Requirements

- Users with ad-hoc database access must be blocked from accessing certain sensitive data elements such as Social Security numbers

Commercial Virtual Private Database Solutions

Oracle Database Vault (DV) extends Virtual Private Database features and provides a console.

Oracle Database Vault (DV)	▪ Licensing per processor ▪ $ 11,500 per processor license ▪ $ 2,530 per processor support and maintenance

Pricing is from the Oracle Technology Global Price List (12/16). Actual cost will vary based on implementation, number of databases, and discounts.

Oracle Database Editions – Security Features

	Express	Standard One	Standard	Enterprise
Data Masking – Redaction				Option
Real Application Security				✓
Oracle Database Vault				Option
Oracle Advanced Security				Option
Oracle Label Security				Option
Secure Application Roles				Option
Oracle Virtual Private Database (VPD)				✓
Fine-Grained Auditing				✓
Proxy Authentication		✓	✓	✓
Data Encryption Toolkit	✓	✓	✓	✓

Virtual Private Database

- **Virtual Private Database (VPD) implements fine-grained access controls (FGAC) for the database.**
  - Allows for row-level security (RLS) and column sensitive policies.
  - Use `DBMS_RLS` package to add, modify, or remove VPD policies.
  - Policies can reference applications contexts and/or PL/SQL functions.
  - Modifies the query being executed and appends to the `WHERE` clause.

Virtual Private Database – Subset

```
BEGIN

  DBMS_RLS.ADD_POLICY (
    'HR',                          -- Schema
    'EMPLOYEES',                   -- Object/table
    'EMP_POLICY',                  -- Policy name
    'HR',                          -- Function schema
    'EMP_SEC',                     -- Function to be called
    'SELECT'                       -- Statement to call policy for
    );
END;
```

User enters the query – **`SELECT * FROM hr.employees;`**

VPD calls the HR.EMP_SEC which returns a where clause predicate. The query is dynamically modified as follows –

```
SELECT * FROM hr.employees WHERE org_id = 1;
```

Virtual Private Database – Hide SSN

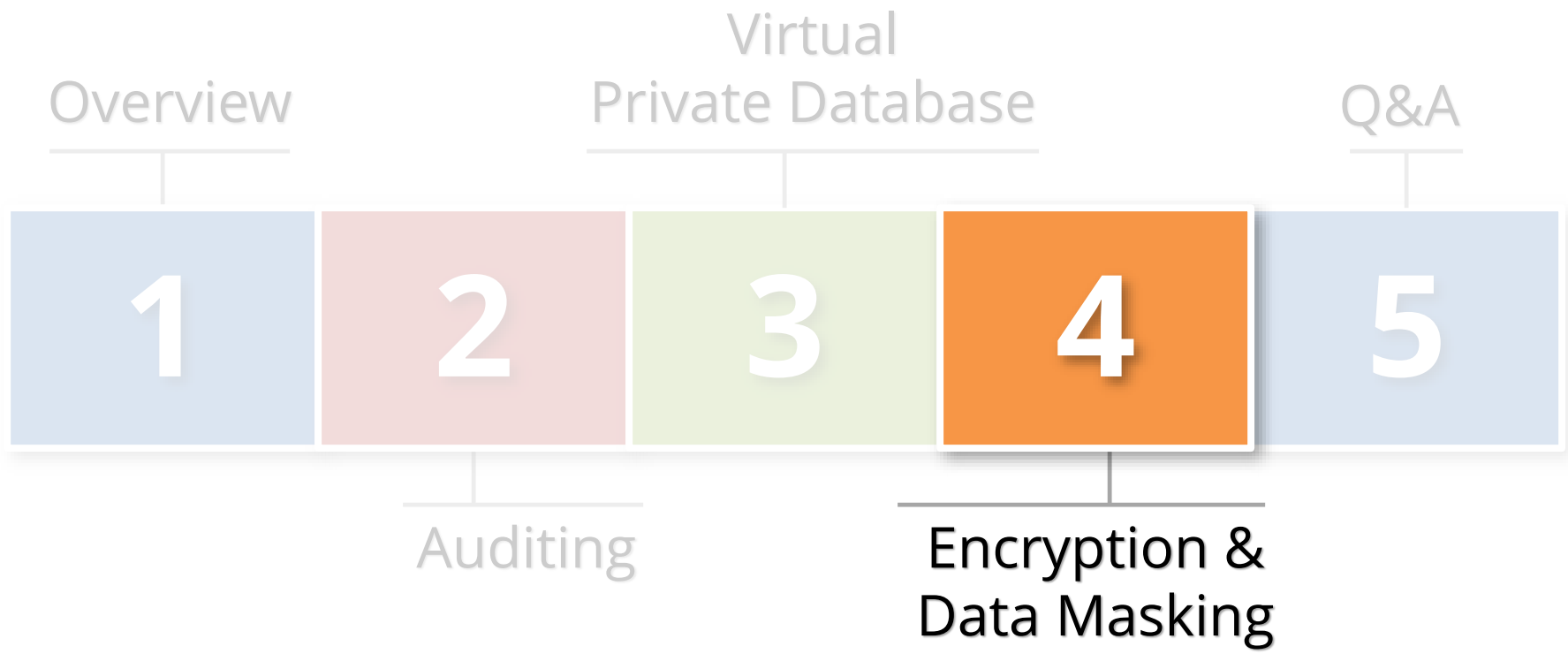
```
BEGIN

  DBMS_RLS.ADD_POLICY (
    object_schema =>             'HR',
    object_name =>               'EMPLOYEES',
    policy_name =>               'EMP_POLICY_SS',
    policy_function =>           'EMP_SEC',
    sec_relevant_cols =>         'NATIONAL_IDENTIFIER',
    sec_relevant_cols_opt =>     'DBMS_RLS.ALL_ROWS'
    );
END;
```

User enters the query – **`SELECT * FROM hr.employees;`**

VPD calls the HR.EMP_SEC and all rows are returned, but the NATIONAL_IDENTIFIER column is masked and only nulls are returned for this column.

Agenda


Overview
Virtual
Private Database
Q&A
1
2
3
4
5
Auditing
Encryption &
Data Masking

Encryption Requirements

- **Sensitive data elements such as Social Security numbers (SSN) and credit card numbers must be –**
  - Encrypted on disk
  - Encrypted on backup media
  - Encrypted when transmitted across network

Commercial Database Encryption Solutions

There are multiple ways to encrypt data in an Oracle Database. The most well-known is Oracle Transparent Data Encryption (TDE).

Oracle Transparent Data Encryption (TDE)	▪ Requires Oracle Advanced Security Option (ASO) ▪ Licensing per processor ▪ $ 15,000 per processor license ▪ $ 3,300 per processor support and maintenance
Vormetric	▪ $ 35,000 Data Security Manager appliance ▪ $ 6,000 per data encryption agent (per database)

Pricing is from the Oracle Technology Global Price List (12/16) and other sources. Actual cost will vary based on implementation, number of databases, and discounts.

Oracle Database Encryption Solutions

Application (access ~ role)	▪ **Database Encryption API (DBMS_CRYPTO)** ▪ Native application encryption
Database (access ~ db account)	▪ **View/Trigger Encryption**
Disk/Storage (access = database)	▪ **Transparent Data Encryption (Oracle TDE)** ▪ Third-party Solutions (e.g., Vormetric) ▪ Disk/SAN Vendor Encryption Solutions ▪ Backup Encryption (e.g., RMAN)

Data in Use

Data at Rest

Data in Use Encryption Solutions

Application (access ~ role)	▪ Application encrypts and decrypts when reading and writing data ▪ Uses standard or custom encryption routines ▪ Encryption routines check security
Database (access ~ db account)	▪ View/Trigger Encryption Solution ▪ View used when reading data ▪ Trigger used when writing data ▪ Calls encryption routines which check security

Data in Use Encryption Solutions

Oracle Database	▪ **DBMS_CRYPTO**
	  ▪ Supports most major encryption and hash algorithms
	  ▪ New database versions add newer encryption and hash algorithms
	  ▪ No key management
	▪ **DBMS_OBFUSCATION_TOOLKIT**
	  ▪ Deprecated and should not be used

Third Party	▪ **Voltage API** ▪ Format preserving encryption ▪ **Vormetric API** ▪ Many others such as OPENSSL, etc.

DBMS_CRYPTO

- **DBMS_CRYPTO is a standard Oracle PL/SQL package that support industry standard encryption and hash algorithms**
  - Encryption = AES, 3DES
  - Hashing = SHA-1, MD5, MD4
  - Replaced DBMS_OBFUSCATION_TOOLKIT package
- **Application calls DBMS_CRYPTO package to encrypt and decrypt data as necessary.**

Encryption Key Management

- **Key management is critical**
  - Do not hard-code encryption keys in a wrapped PL/SQL package or table
  - Keys must be properly protected, rotated, and managed
- **Many organizations have a key management infrastructure that can be utilized –**
  - Hardware security module – SafeNet, RSA, etc.
  - Key management server – Oracle, Vault by HashiCorp (free)
- **Requires PL/SQL or Java code to access API**

Network Encryption

Application Server or Client
 	
← →
 	
Database Server
 	
(SQL*Net)
	SQL*Net Encryption
	▪ Formerly part of Advanced Security Option
	▪ **Now included with Oracle Database Enterprise Edition**
	
	▪ Encrypts all SQL*Net database traffic
	▪ Supports
	  ▪ AES (128, 192, 256) – outer CBC only
	  ▪ 3DES (112, 168) – CBC only
	
	▪ Data integrity supported using MD5 or SHA-1

SQL*Net Encryption

- **Database Server Side**
  - $ORACLE_HOME/network/admin/sqlnet.ora

```
SQLNET.ENCRYPTION_SERVER=requested or required
SQLNET.ENCRYPTION_TYPES_SERVER=(AES128, AES256)
SQLNET.CRYPTO_CHECKSUM_SERVER=required or required
SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER=(sha1)
```

- **Encryption algorithms may have to be tweaked as older client installations will only support older algorithms**
  - Review algorithms as weak and outdated algorithms are still supported in Oracle

SQL*Net Encryption Negotiation

Client Setting	Server Setting	Encryption Result
REJECTED	REJECTED	OFF
ACCEPTED *	REJECTED	OFF
REQUESTED	REJECTED	OFF
REQUIRED	REJECTED	Connection fails
REJECTED	ACCEPTED *	OFF
ACCEPTED *	**ACCEPTED ***	**OFF***
REQUESTED	ACCEPTED *	ON
REQUIRED	ACCEPTED *	ON
REJECTED	REQUESTED	OFF
ACCEPTED *	REQUESTED	ON
REQUESTED	REQUESTED	ON
REQUIRED	REQUESTED	ON
REJECTED	REQUIRED	Connection fails
ACCEPTED *	REQUIRED	ON
REQUESTED	REQUIRED	ON
REQUIRED	REQUIRED	ON

* Default

Auditing SQL*Net Encryption

- **Can check in the database if connections are using encryption**
  - Do not know what encryption algorithm is being used

```
select NETWORK_SERVICE_BANNER
from v$session_connect_info
```

```
NETWORK_SERVICE_BANNER
----------------------------------------------------------------------------------------------------
Windows NT TCP/IP NT Protocol Adapter for 32-bit Windows: Version 11.2.0.2.0 - Production
Oracle Advanced Security: encryption service for 32-bit Windows: Version 11.2.0.2.0 - Production
Oracle Advanced Security: crypto-checksumming service for 32-bit Windows: Version 11.2.0.2.0 – Prod
```

Data Masking and Reaction Requirements

- Sensitive data elements such as Social Security numbers (SSN) and credit card numbers must be masked or scrambled in development and test databases
- Sensitive data elements such as Social Security numbers and credit card numbers must be masked when displayed to the user based on database privileges

Commercial Data Masking and Redaction Solutions

Oracle provides two add-on solutions for data masking and redaction.

Oracle Data Redaction	▪ Requires Oracle Advanced Security Option (ASO) ▪ Licensing per processor ▪ $ 15,000 per processor license ▪ $ 3,300 per processor support and maintenance
Oracle Data Masking Pack	▪ Requires Oracle Enterprise Manager (OEM) ▪ Licensing per processor ▪ $ 11,500 per processor license ▪ $ 2,530 per processor support and maintenance

Pricing is from the Oracle Technology Global Price List (12/16). Actual cost will vary based on implementation, number of databases, and discounts.

Data Masking/Scrambling Options

- **SQL scripts**
  - Most instances a simple SQL script will suffice
  - Use when data integrity and consistency across tables is not required
  - Performance not as good as commercial solutions
- **Solix Enterprise Data Management Suite – Standard Edition Data Masking**
  - Free version of the Solix Suite

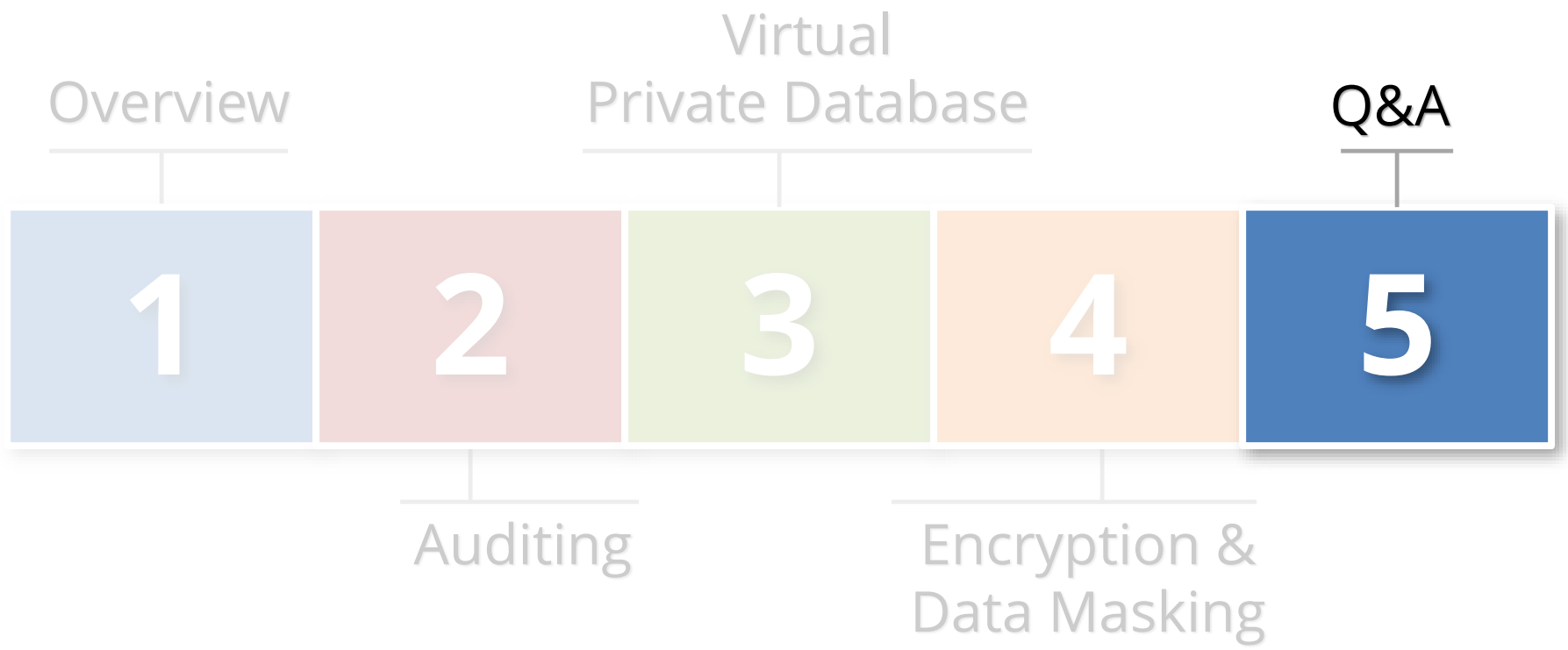
Redaction Options

- **Use Views for custom applications**
  - Simple and very effective solution
  - Must be able to modify application
- **VPD/FGAC can be used to return null for columns**
  - Often the data element does not have to be masked, but removed from the result set

Transparent Sensitive Data Protection

- **Transparent Sensitive Data Protection (TSDP) is a new 12.1 feature that maintains an inventory of sensitive data and integrates with VPD (Enterprise Edition) and Reaction (ASO license)**
  - Included with Enterprise Edition
- **Use with custom scripts and FGAC**

Agenda


Overview
Virtual
Private Database
Q&A
1
2
3
4
5
Auditing
Encryption &
Data Masking

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**