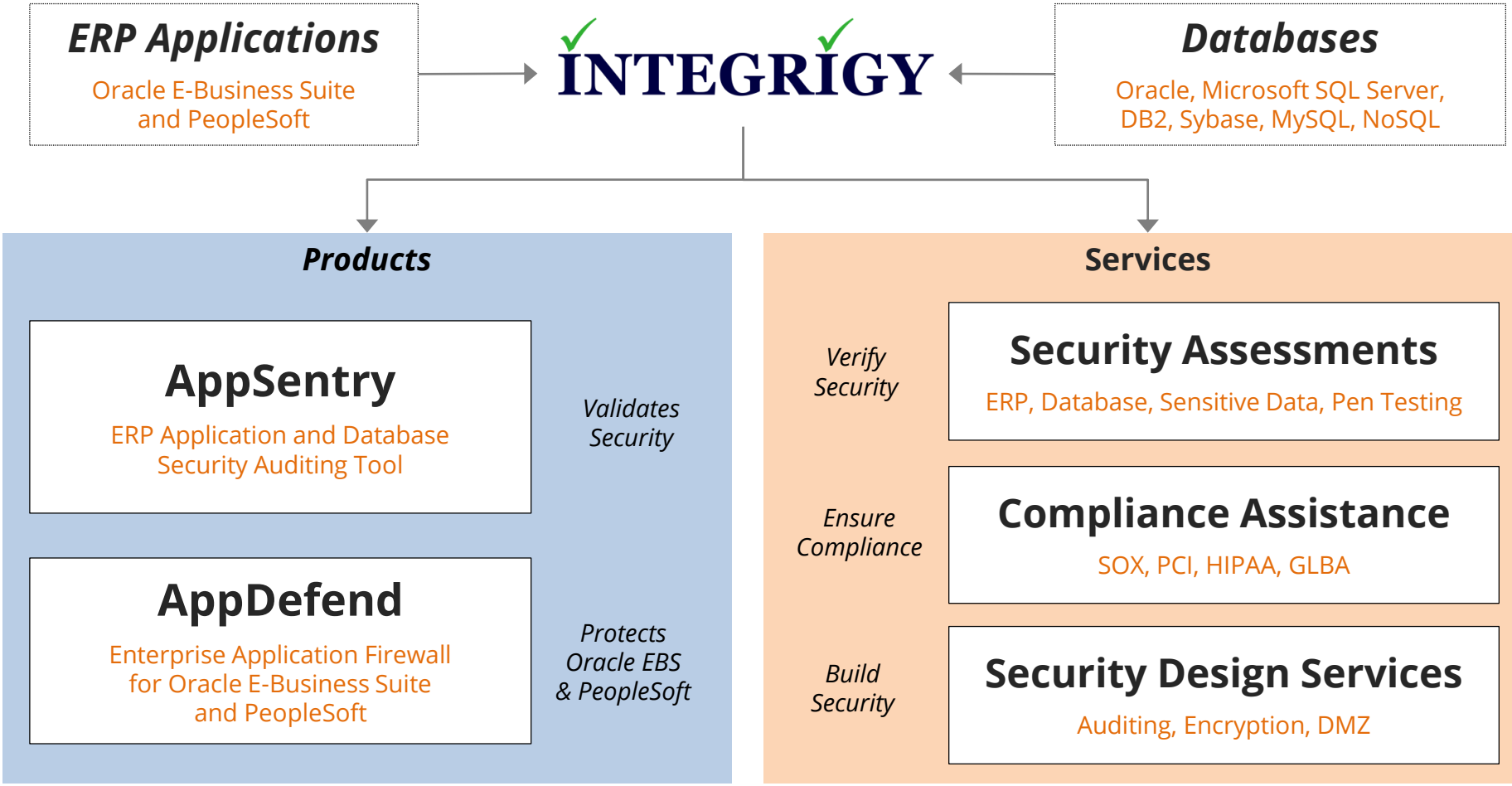
Is Your Sensitive Data Playing Hide and Seek with You?

December 12, 2019

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

About Integrigy



Agenda

1. Sensitive Data Overview
2. Sensitive Data Locations
3. Sensitive Data Discovery
4. Sensitive Data Protection
5. Q & A

Agenda

1. Sensitive Data Overview
2. Sensitive Data Locations
3. Sensitive Data Discovery
4. Sensitive Data Protection
5. Q & A

Sensitive Data Drivers – Compliance

- **PCI (Payment Card Industry - Data Security Standard)**
  - Must encrypt credit card numbers
- **GDPR (General Data Protection Regulation**
  - Protection of individual personal information
  - Broad regulation regarding control, access, retention of personal information
- **HIPAA (Health Insurance Portability and Accountability Act)**
  - Electronic Protected Health Information (ePHI) should be encrypted – an addressable implementation specification
  - Breach regulations exclude encrypted data

Sensitive Data Drivers – State Privacy Laws

- **Privacy Laws (National/State Regulations)**
  - Read access to sensitive data such as national identifiers and bank account numbers
  - Breach regulations often specifically exclude encrypted data (NY, MA, NJ, MD, OR, TX, WA)
- **California Consumer Privacy Act (CCPA)**
  - Effective January 2020
- **Maine Act to Protect the Privacy of Online Consumer Information**
  - Effective July 2020
  - Requires reasonable measures to protect consumer information

What is Sensitive Data?

Payment Card Industry Data Security Standard (PCI-DSS 3.2)	▪ Credit Card Number
	  ▪ *Primary Account Number (PAN)*
	▪ CVV/CV2/CID
	  ▪ *3 digits on the back for Visa/MC*
	  ▪ *4 digits on the front for AMEX*
	▪ Magnetic Stripe Data (very rare in applications)

Privacy Regulations (employees, customers, vendors)	▪ First and last name
	▪ Plus one of the following:
	  ▪ Social security number (SSN, Tax ID, 1099)
	  ▪ Credit card number
	  ▪ Bank account number
	  ▪ Financial account number
	  ▪ Driver license or state ID number

HIPAA (Privacy Standard and Security Rule)	▪ First and last name
	▪ Plus one of the following (Protected Health Information)
	  ▪ “the past, present, or future physical or mental health, or condition of an individual”
	  ▪ “provision of health care to an individual”
	  ▪ “payment for the provision of health care to an individual”

Agenda

1. Sensitive Data Overview
2. **Sensitive Data Locations**
3. Sensitive Data Discovery
4. Sensitive Data Protection
5. Q & A

Examples of Sensitive Data Locations

Sensitive Data Elements	Common Application Elements
Credit Card Number	Customer
	Employee Corporate Card
Social Security Number	Employee
	Vendor Tax ID/1099
	Customer
Bank Account Number	Company Bank Account
	Employee Bank Account (direct deposit)
	Vendor Bank Account

Where is Sensitive Data in Oracle E-Business Suite?

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) (1099)	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
Electronic Protected Health Information (ePHI)	Order Management Accounts Receivables Human Resources

Sensitive Data Elements in EBS

Sensitive Data Element	Most Common Data Types	EBS Module	EBS Native Encryption
Credit Card Number	**Customer**	OM/AR/IBY	**11i and R12**
	Employee Corporate Card	AP/IBY/iExp	**R12**
Social Security Number	**Employee**	HR	No
	Vendor Tax ID/1099	AP	No
	Customer	AR/Custom	No
Bank Account Number	**Company Bank Account**	CE	No
	Employee Bank Account (direct deposit)	HR	No
	Vendor Bank Account	AP/IBY	**R12**

Where else might be Sensitive Data? (EBS)

- **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_DEC122019
- **Interface tables**
  - Credit card numbers are often accepted in external applications and sent to Oracle EBS or processed using XML Gateway
- **Oracle EBS Flexfields**
  - It happens – very hard to find

Database

- **Interface files**
  - Flat files used for interfaces or batch processing
- **Log files**
  - Log files generated by the application (e.g., Oracle Payments)

File System

Transient Sensitive Data Locations

```
insert into PII_DATA (FIRST_NAME, LAST_NAME, SSN, DOB)
values ('JANE', 'JONES', '987-65-4321','12/31/1990');
```

Data Dictionary	▪ V$SQL ▪ V$SQL_BIND_DATA (bind values)
Audit Trail	▪ If auditing is enabled for table (object), role, or system privilege AND auditing is set to “extended”
Trace Files	▪ If tracing enabled for session ▪ Bind variables only if tracing is specifically set to capture bind variables

Agenda

1. Sensitive Data Overview
2. Sensitive Data Locations
3. **Sensitive Data Discovery**
4. Sensitive Data Protection
5. Q & A

Sensitive Data Discovery

- **Detailed sensitive data inventory should be maintained**
  - Must be updated periodically
  - Work with development teams and DBAs to identify new locations
- **Do not rely solely on column names to find sensitive data**
  - Column names are very unreliable
  - No standard naming conventions
  - Data may be in multi-use columns such as Oracle EBS Flexfields
- **Use an automated tool to periodically scan for sensitive data**
  - Oracle DBSAT – Discoverer
  - Oracle Enterprise Manager – Quality Management -> Data Discovery
  - Oracle Cloud Data Safe – Data Discovery
  - Integrigy AppSentry Sensitive Data Discovery

AppSentry Sensitive Data Discovery (SDD)

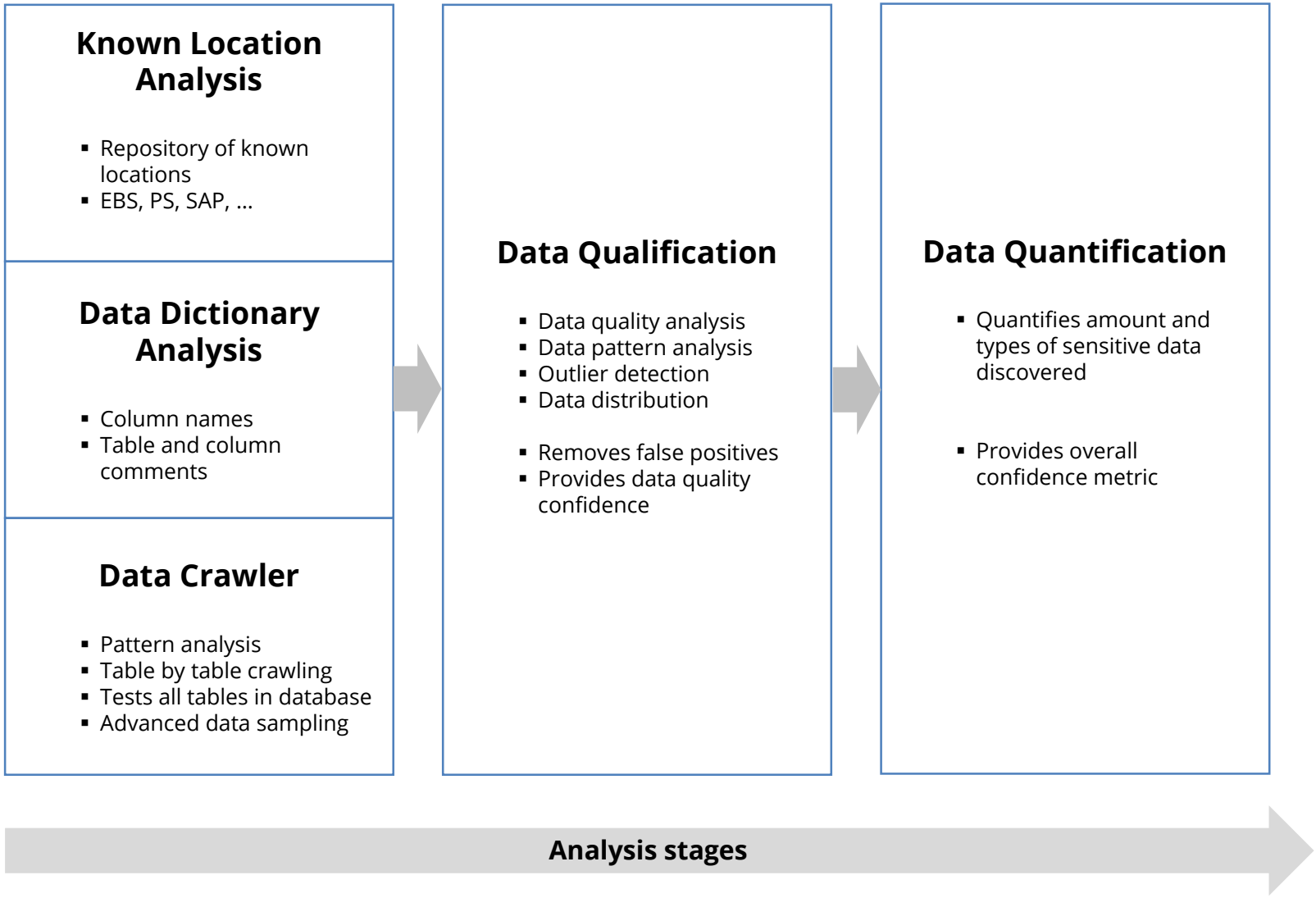


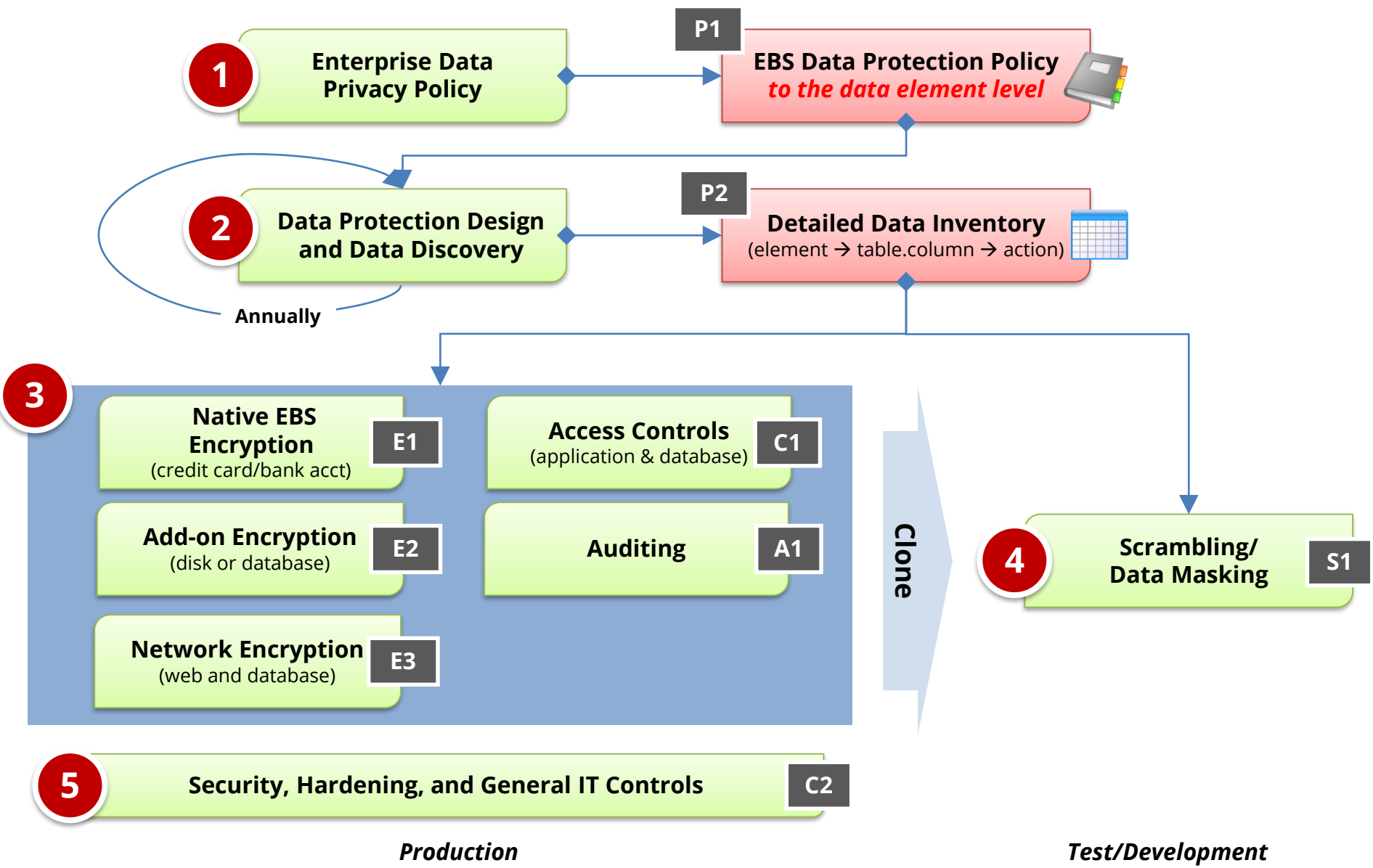
Table and Column Comments

- **Table and column comments are not frequently used by package or custom applications**
  - Applications often support multiple databases
  - Table and column comments are not ANSI SQL
  - Comments not required by most development standards
- **Oracle E-Business Suite**
  - Tables = 1,134 out of 23,036 (5%) have comments
  - Columns = 23,784 of 1,972,592 (1%) have comments
- **Oracle PeopleSoft**
  - No table comments
  - No column comments

Agenda

1. Sensitive Data Overview
2. Sensitive Data Locations
3. Sensitive Data Discovery
4. **Sensitive Data Protection**
5. Q & A

Integrigy Sensitive Data Protection Process



Oracle EBS Sensitive Data Encryption

Sensitive Data Element	Most Common Data Types	EBS Module	EBS Native Encryption
Credit Card Number	**Customer**	OM/AR/IBY	**11i and R12**
	Employee Corporate Card	AP/IBY/iExp	**R12**
Social Security Number	**Employee**	HR	No
	Vendor Tax ID/1099	AP	No
	Customer	AR/Custom	No
Bank Account Number	**Company Bank Account**	CE	No
	Employee Bank Account (direct deposit)	HR	No
	Vendor Bank Account	AP/IBY	**R12**

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

TDE Encryption Misconceptions

- **Not an access control tool**
  - Encryption does not solve access control problems
  - Data is encrypted the same regardless of user
- **Malicious employee protection**
  - Encryption does not protect against malicious privileged employees and contractors
  - DBAs have full access
- **More is not better**
  - Performance cost of encryption
  - Cannot encrypt everything

Column vs. Tablespace Encryption (Sample)

- **Column encryption**
  - Fairly straight forward for simple cases such as NATIONAL_IDENTIFIER in HR.PER_ALL_PEOPLE_F
  - Encryption done in place using ALTER TABLE
  - Do not use SALT if column is indexed
  - Use for standard applications columns
  - Increases storage for each value between 1 and 52 bytes

- **Tablespace encryption**
  - Tablespace encryption supported starting with 11g
  - Tablespace must be exported and imported to implement encryption
  - Use for custom tablespaces or entire database

Transparent Sensitive Data Protection (TSDP)

- **Transparent Sensitive Data Protection (TSDP)**
  - Introduced with Oracle 12c
  - Requires Enterprise Edition
- **Use TSDP to identify, create and manage policies to protect sensitive data. Use with –**
  - Oracle Data Redaction
  - Oracle Virtual Private Database (VPD)
  - Unified Auditing
  - Fine-grained Auditing (FGA)
  - Transparent Data Encryption (TDE) column encryption

Integrigy 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**