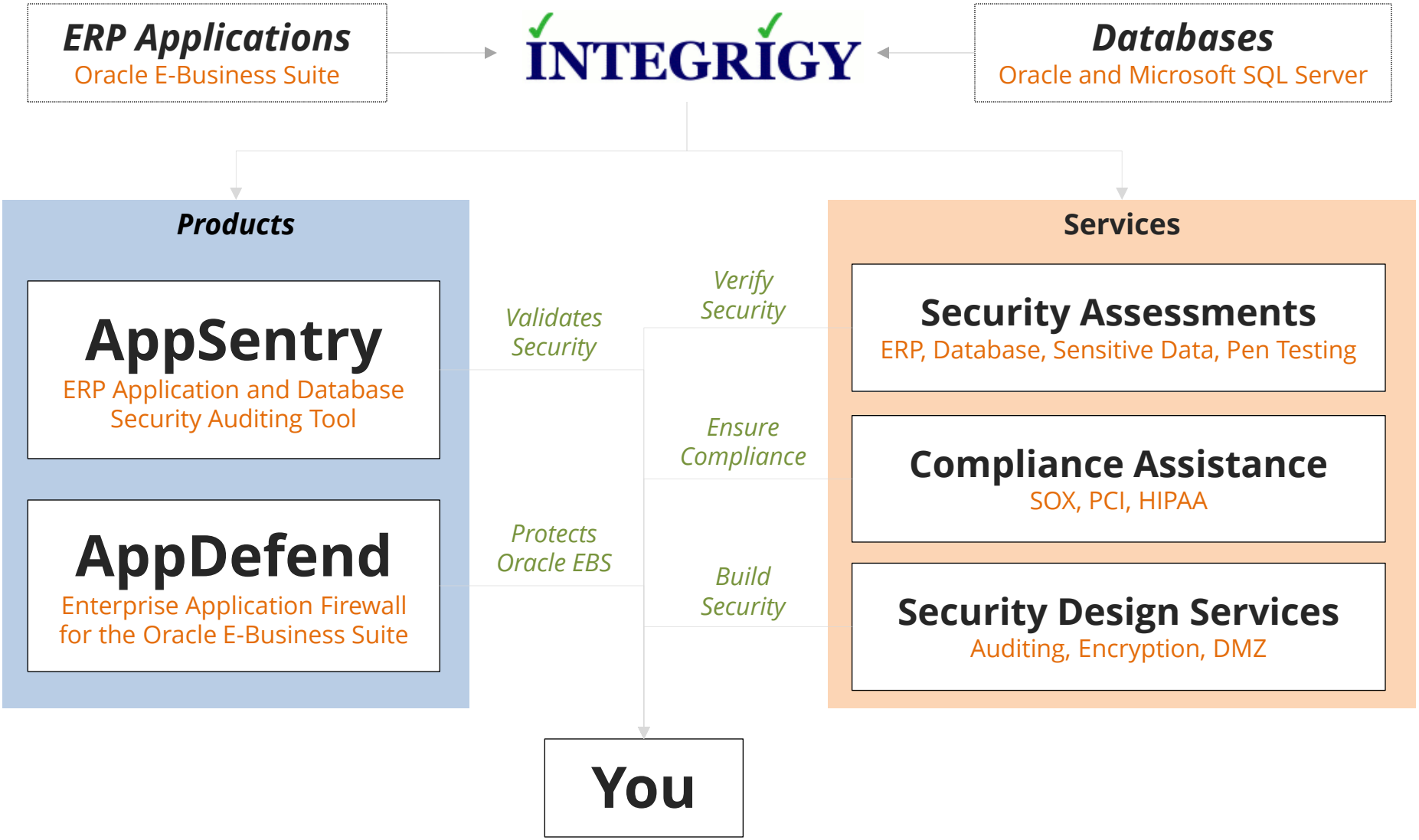
Encrypting Sensitive Data in Oracle E-Business Suite

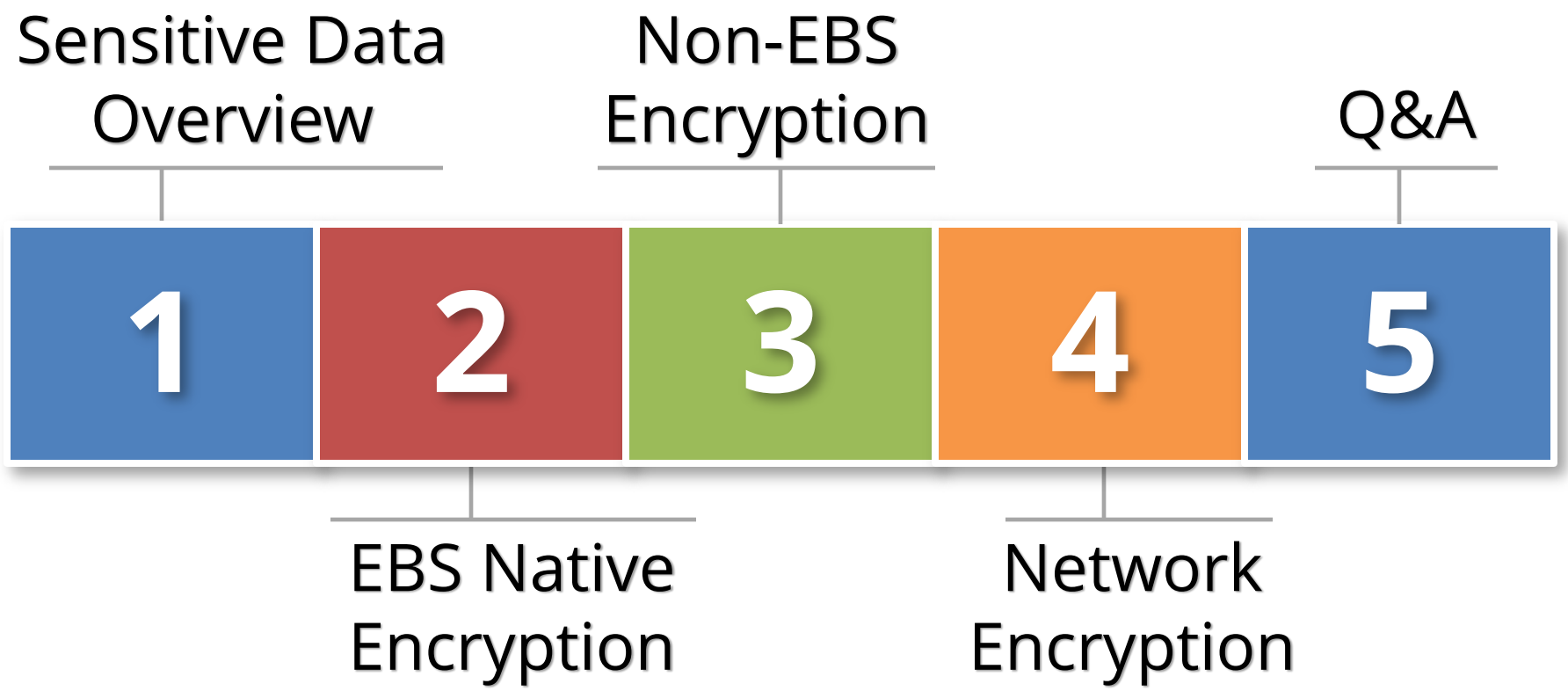
December 19, 2013

Stephen Kost
Chief Technology Officer
Integrigy Corporation

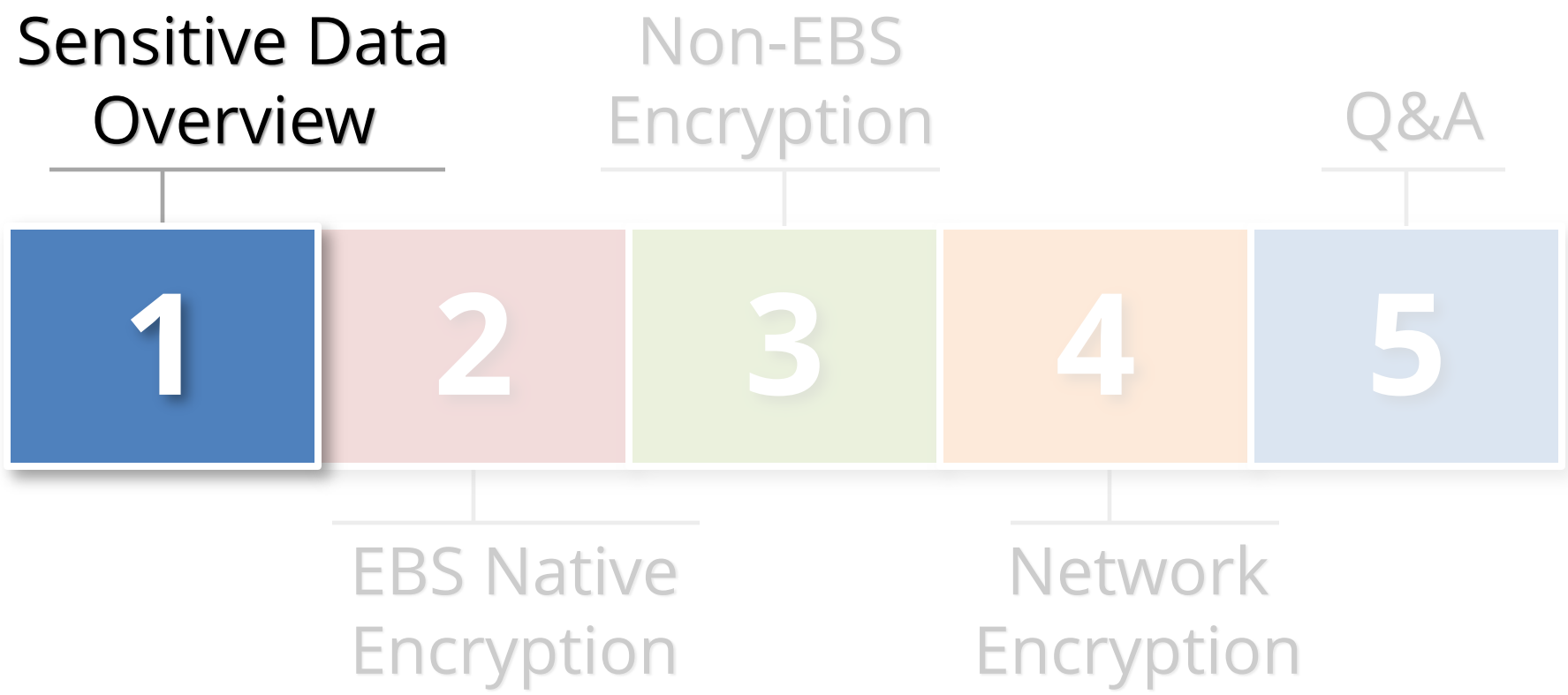
About Integrigy



Agenda


Sensitive Data Overview
Non-EBS Encryption
Q&A
1
2
3
4
5
EBS Native Encryption
Network Encryption

Agenda


Sensitive Data Overview
Non-EBS Encryption
Q&A
1
2
3
4
5
EBS Native Encryption
Network Encryption

Why – Sensitive Data Encryption Drivers

- **PCI** ***(Payment Card Industry - Data Security Standard)***
  - Must encrypt credit card numbers
- **Privacy Laws** ***(National/State Regulations)***
  - Read access to sensitive data (National Identifier and Bank Account Number)
  - Breach regulations often specifically exclude encrypted data
  - California (SB 1386) and Massachusetts data privacy laws
- **HIPAA** ***(Health Insurance Portability and Accountability Act)***
  - Electronic Protected Health Information (ePHI) should be encrypted – an addressable implementation specification
  - Breach regulations exclude encrypted data

What is Sensitive Data in Oracle EBS?

Payment Card Industry Data Security Standard (PCI-DSS 3.0)	▪ 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 EBS)

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”

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)
(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

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 or processed using XML Gateway

Oracle EBS Flexfields

- It happens – very hard to find

Database

Interface files

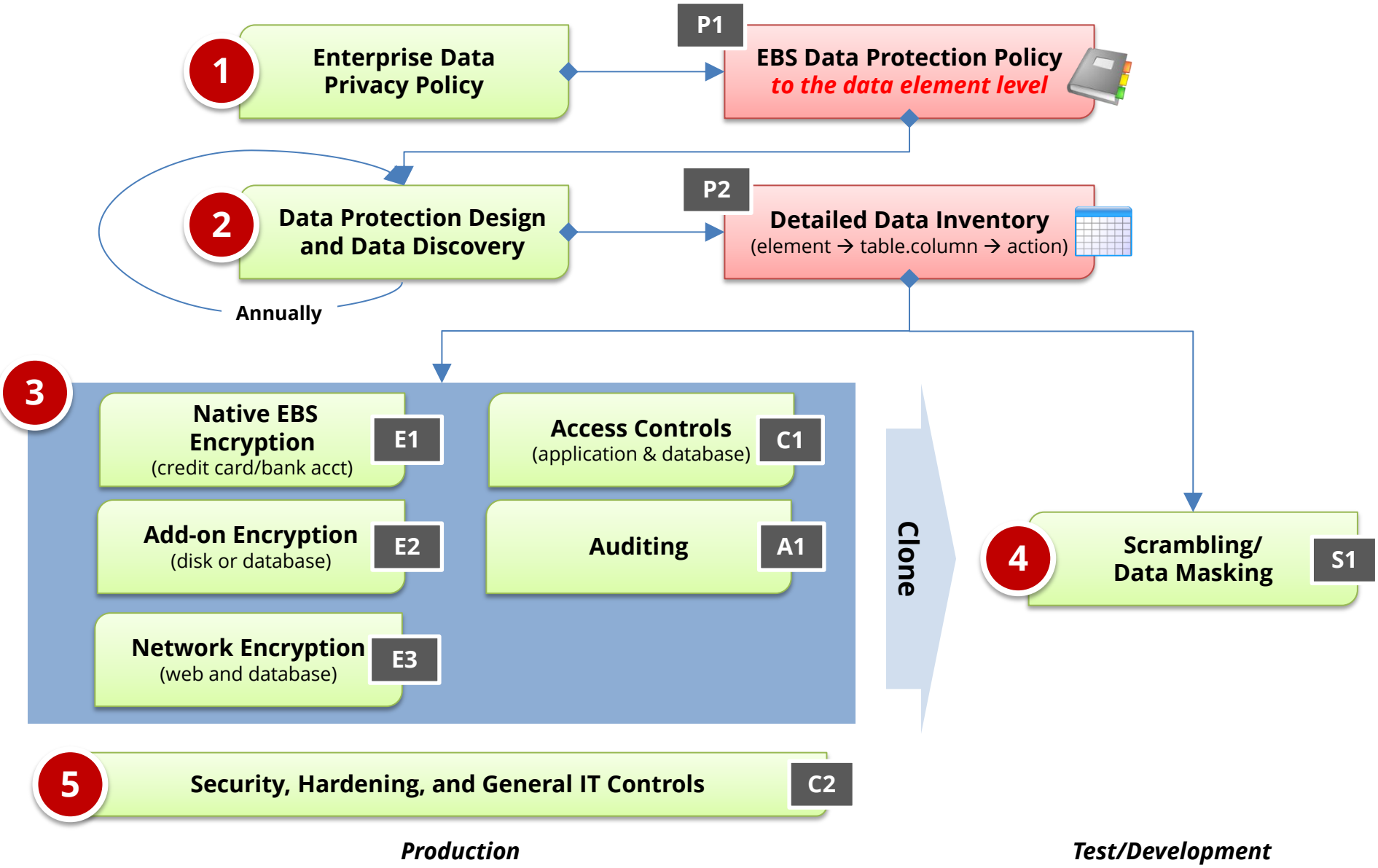
- Flat files used for interfaces or batch processing

Log files

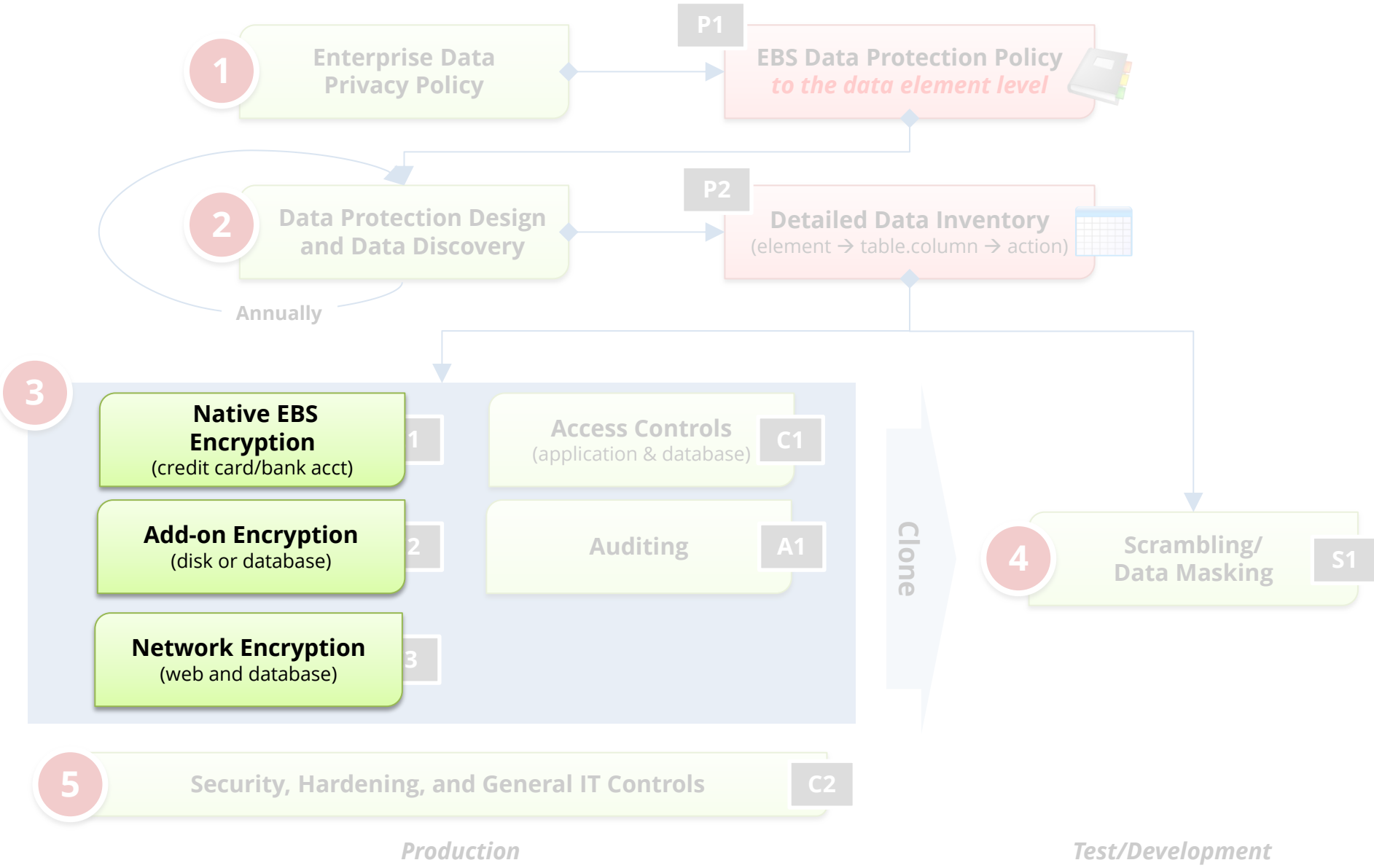
- Log files generated by the application (e.g., Oracle Payments)

File System

How – Integrigy EBS Data Protection Process



How – Integrigy EBS Data Protection Process



Types of Encryption

- **Storage (Data at rest)**
  - **Disk, storage, media level encryption**
  - Encryption of data at rest such as when stored in files or on media
- **Network (Data in motion)**
  - **Encryption of data when transferred between two systems**
  - SSL/HTTPS (users) and SQL*Net encryption (database)
- **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

Storage/Access Oracle EBS Encryption Solutions

Application (access = responsibility)	▪ **Oracle EBS Credit Card Number Encryption** ▪ Encryption for Customizations (DBMS_CRYPTO/FND_VAULT)
Database (access = db account)	▪ View/Trigger Encryption for Customizations
Disk/Storage (access = database)	▪ **Oracle Transparent Data Encryption (TDE)** ▪ Third-party Solutions (e.g., Vormetric) ▪ Disk/SAN Vendor Encryption Solutions ▪ Backup Encryption (e.g., RMAN)

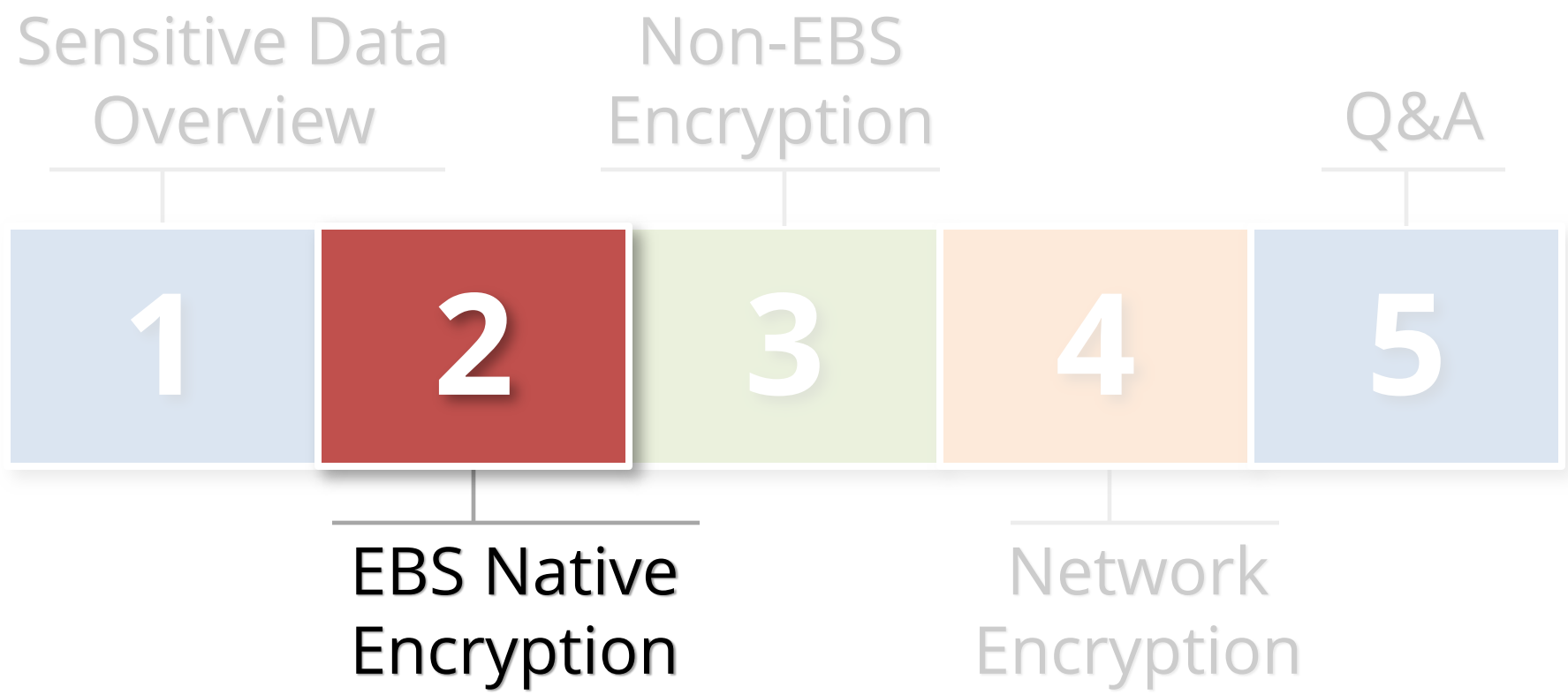
Network Oracle EBS Encryption Solutions

User ↔ Application Server (http)	▪ **Native EBS SSL Encryption** ▪ **SSL Endpoint** – Use a load balancer or reverse proxy
Application Server ↔ Database Server (SQL*Net)	▪ **SQL*Net Encryption** – Formerly part of Advanced Security Option – Now included with Oracle EBS Database

Big 3 Sensitive Data Elements in EBS

Sensitive Data Element	Most Common Data Types	EBS Module	EBS Native Encryption
Credit Card Number	**Customer**	OM/AR/IBY	Optional
	Employee Corporate Card	AP/IBY/iExp	Optional
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	Optional

Agenda


Sensitive Data Overview
Non-EBS Encryption
Q&A
1
2
3
4
5
EBS Native Encryption
Network Encryption

Oracle EBS Native Encryption

Oracle E-Business Suite includes **native application-level encryption** for a limited set of fields based on version and module.

- **Not enabled by default in 11i or R12**
- 11i = general patch release availability October 2006
- R12 = included with base R12 release
- Significantly better solution than TDE or disk level encryption

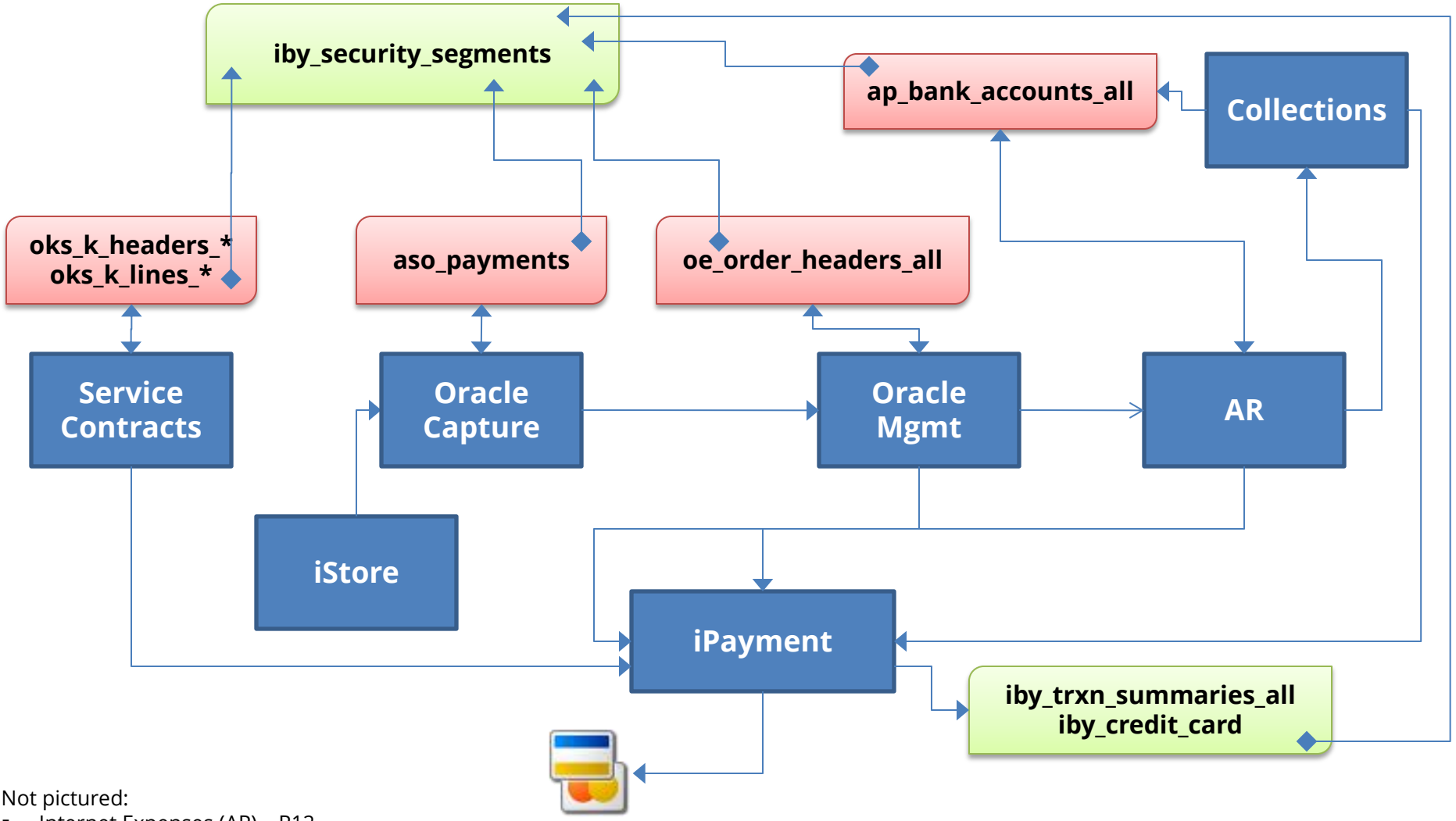
Big 3 Sensitive Data Elements in EBS

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**

Oracle EBS Native Encryption

11i	▪ **MOS Note ID 338756.1 – Patch 4607647** ▪ Significant functional pre-requisites (11.5.10.2) ▪ Only credit card numbers ▪ Keys stored in the database
R12	▪ **MOS Note ID 863053.1** ▪ Credit card numbers and bank account numbers ▪ Uses Oracle Wallet to store encryption keys

Oracle Credit Card Encryption Design



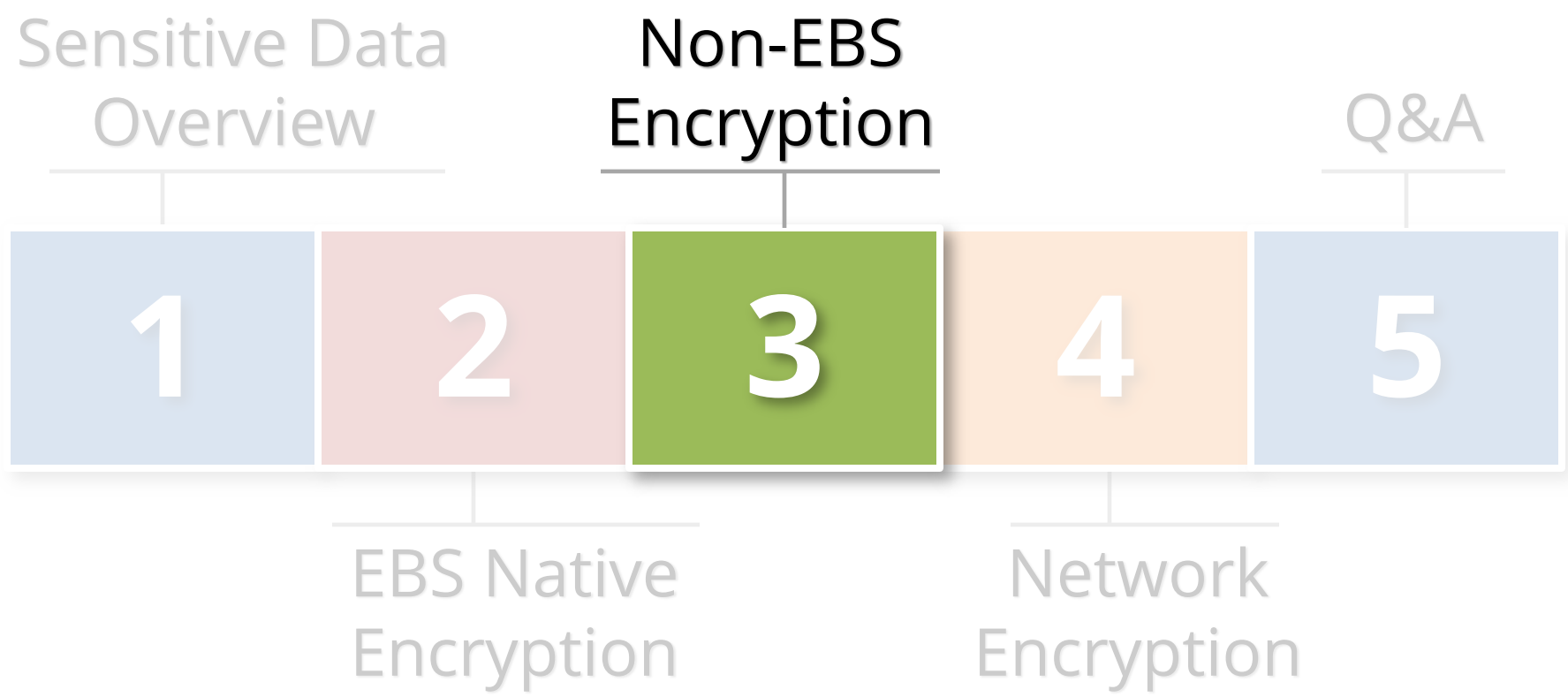
Not pictured:

- Internet Expenses (AP) – R12
- Lease Management (AP) – same as AR
- Student System (IGS) – IGS patch

EBS Native Encryption Challenges

- Encryption keys must be rotated periodically as required by PCI
- No method or supported procedure to purge encrypted data as required by PCI
- Encryption keys must be changed in test and development environments
- For PCI, no live credit card numbers allowed in test and development

Agenda


Sensitive Data Overview
Non-EBS Encryption
Q&A
1
2
3
4
5
EBS Native Encryption
Network Encryption

What is Oracle TDE?

- **Transparent database encryption**
  - Requires no application code or database structure changes to implement
  - Only major change to database function is the Oracle Wallet must be opened during database startup
  - Add-on feature licensed with Advanced Security Option

- **Limited to encrypting only certain columns**
  - Cannot be a foreign key or used in another database constraint
  - Only simple data types like number, varchar, date, …
  - Less than 3,932 bytes in length

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

Data Center Theft

From Chicago Police Report -

- At least two masked intruders entered the suite after cutting into the reinforced walls with a power saw.
- During the robbery, the night manager was repeatedly tazered and struck with a blunt instrument.
- At least 20 data servers were stolen.

Column vs. Tablespace Encryption

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 for Oracle EBS columns
- **Use for standard Oracle EBS columns**

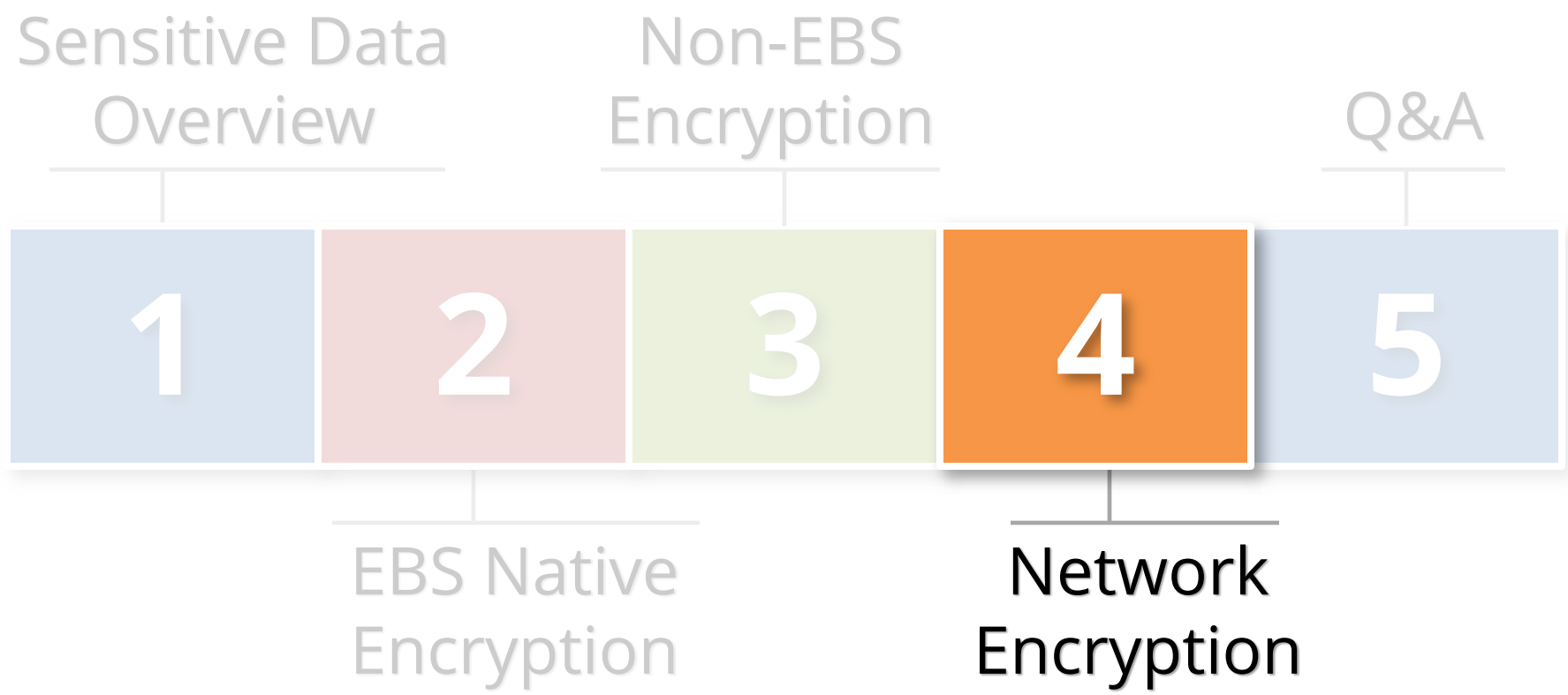
Tablespace encryption

- Tablespace encryption only supported in 11g for 11i/R12
- Tablespace must be exported and imported to implement encryption
- OATM uses large tablespaces (APPS_TS_TX_DATA)
- **Use for custom tablespaces or entire database**

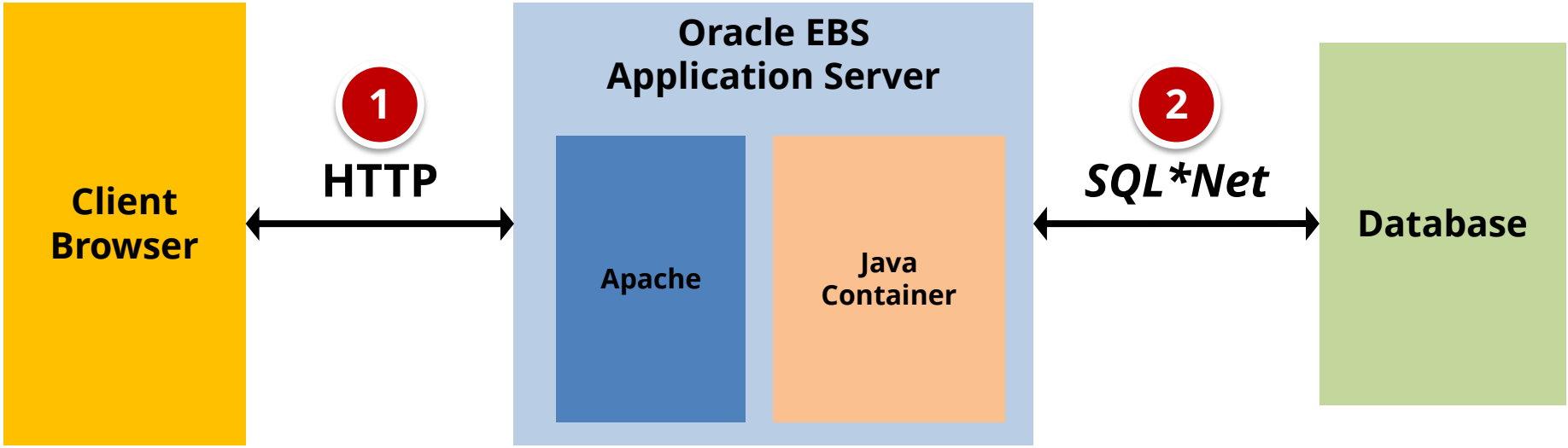
Performance Considerations

- **Impact is limited to CPU performance**
  - Data must be encrypted and decrypted
  - Highly dependent on access patterns to data
- **No disk I/O read or write impact**
  - Change is not significant
- **Column Encryption**
  - 5% to 20% CPU performance impact for several customers
- **Tablespace Encryption**
  - Encrypting entire database is feasible
  - 10% to 15% CPU performance impact for one customer on high transaction volume tables

Agenda

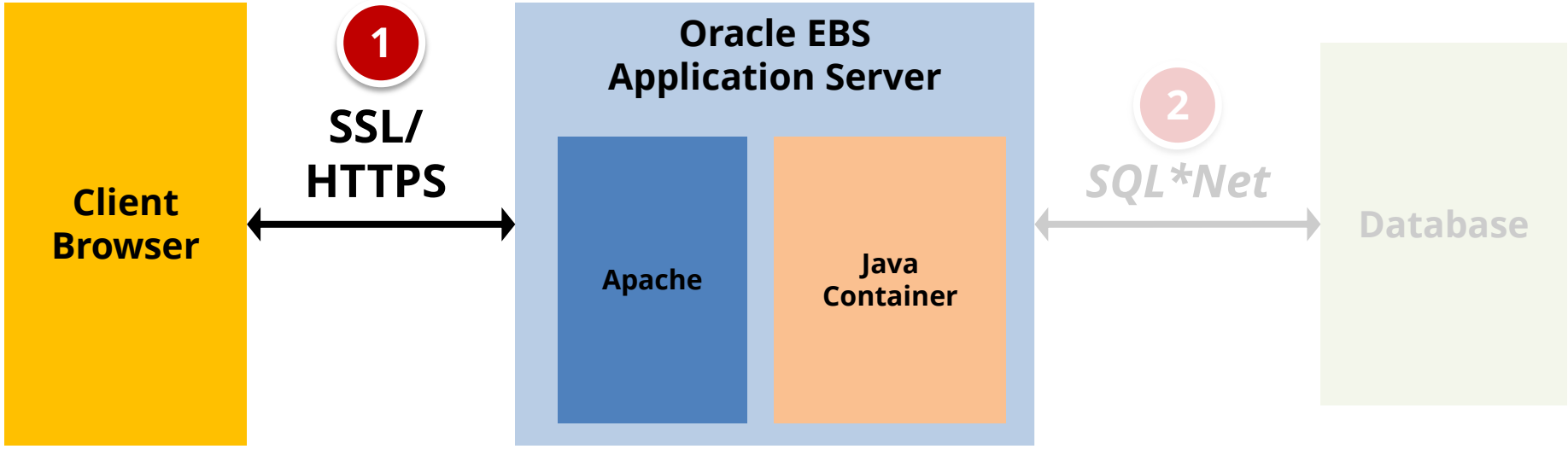

Sensitive Data Overview
Non-EBS Encryption
Q&A
1
2
3
4
5
EBS Native Encryption
Network Encryption

Oracle EBS Default Network Communication



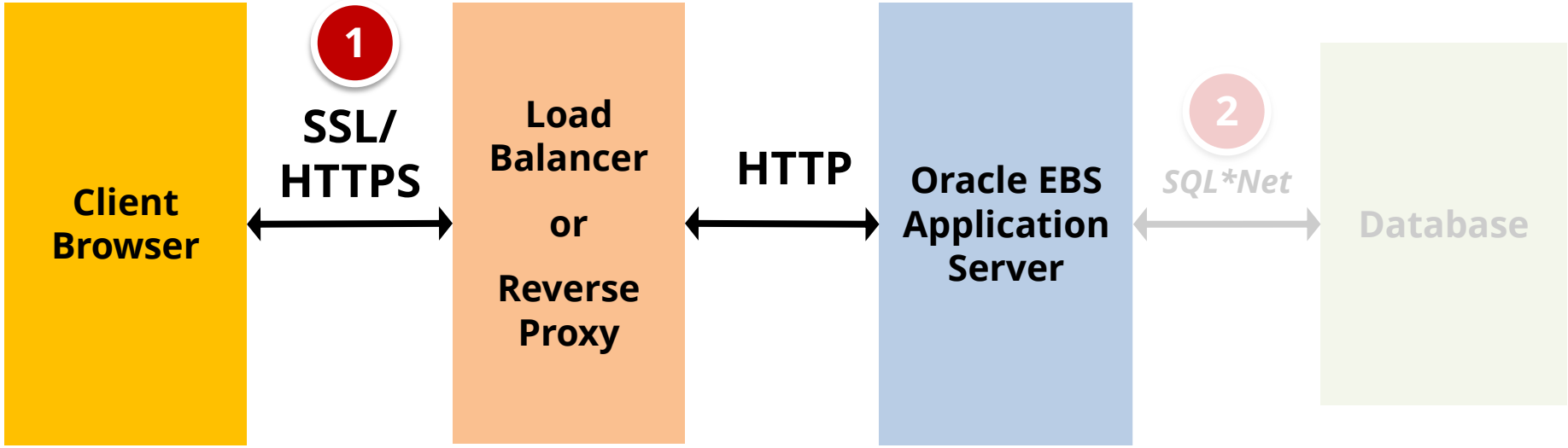
1. Communication from the **client browser** to the **application server** uses the HTTP protocol and all traffic is unencrypted, including passwords.
2. Communication from the **application server** to the **database** uses the Oracle SQL*Net protocol and all traffic is unencrypted, except database passwords.

Client to Application Server (Native)



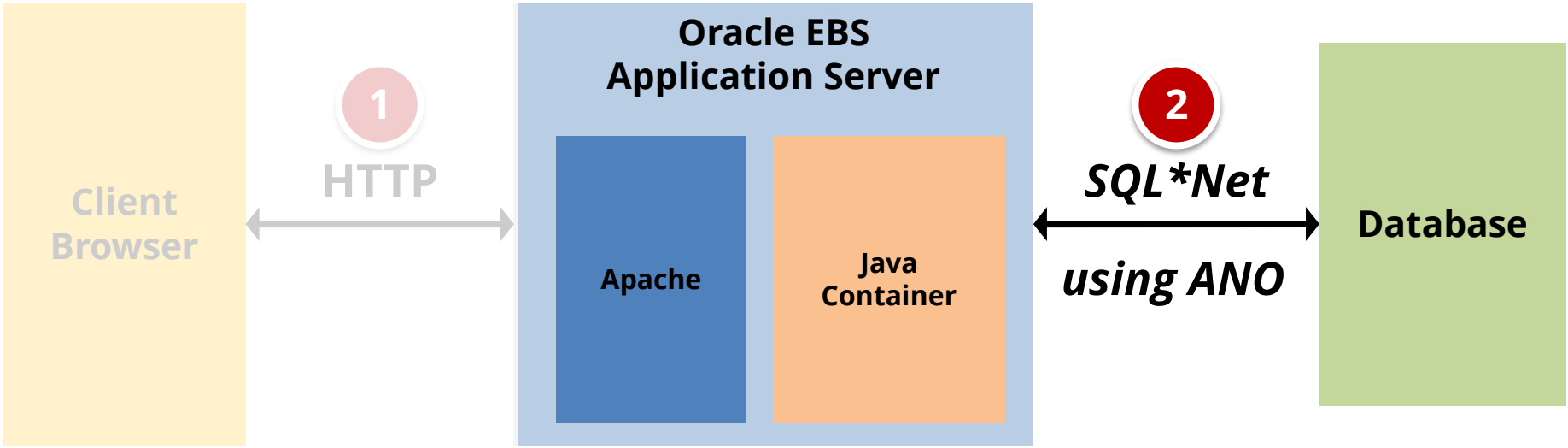
- SSL encryption (just like with your bank uses) should be implemented for Oracle EBS as EBS natively supports SSL. Modify SSL encryption settings to strengthen.
- See My Oracle Support Notes 376700.1 (R12) and 123718.1 (11i).
- Many Oracle EBS implementations will only encrypt external application servers (iSupplier, iStore, etc.).

Client to Application Server (Proxy)



- SSL encryption may be off-loaded to a load balancer (F5 BigIP) or reverse proxy server to centralize the SSL implementation and reduce load on the application server. SSL terminates on the load balancer and communication is HTTP between load balancer and application server.
- See My Oracle Support Notes 380489.1 (R12), 217368.1 (11i) , and 727171.1 for more information.

Application Server to Database Server



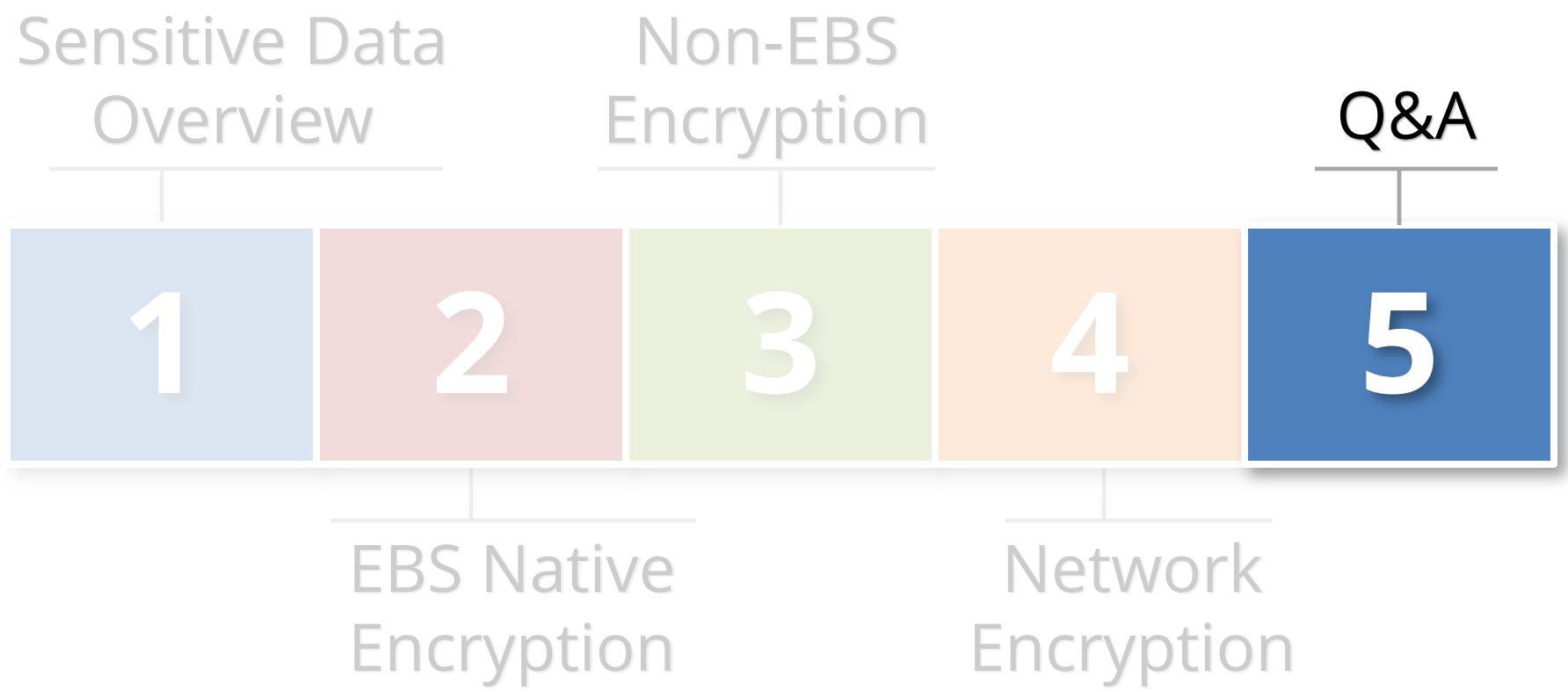
- SQL*Net encryption requires Advanced Networking Option (ANO). ANO is included with the database as of July 2013.
- See My Oracle Support Notes 376700.1 (R12) and 391248.1 (11i) for implementation details.

How - Data Protection vs. Threats

Data Access Method and Threats	Options						
	1 EBS Encrypt	2 Trigger View	3 Oracle TDE	4a FGAC	4b Internal Audit	4c External Audit	3 + 4 TDE + Auditing
1. Application access by end-users (responsibility)	E	E		C	A	A	A
2. Application access by application administrators	E+	E-		C	A	A	A
3. Database access by DBA	E	E		C	A+	A	A
4. Database access by Applications DBA (SYSTEM, APPS)	E+	E+			A+	A+	A+
5. Database access by other database accounts	E	E		C	A	A	A
6. Operating system access to database data files	E	E	E				E
7. On-line or off-line access to database backups	E	E	E				E
8. Exploitation of Oracle Applications security vulnerabilities	E-	E-		C+	A+	A+	A+
9. Exploitation of Oracle Database security vulnerabilities	E+	E+		C+	A+	A+	A+
10. Exploitation of operating system security vulnerabilities	E	E	E				E

E = Encrypted, **C** = Access Controlled, **A** = Access Audited, **+** = Mostly **-** = Partially

Agenda


Sensitive Data Overview
Non-EBS Encryption
Q&A
1
2
3
4
5
EBS Native Encryption
Network Encryption

Contact Information

Stephen Kost
Chief Technology Officer
Integrigy Corporation

web: **www.integrigy.com**
e-mail: **stephen.kost@integrigy.com**
blog: **integrigy.com/oracle-security-blog**