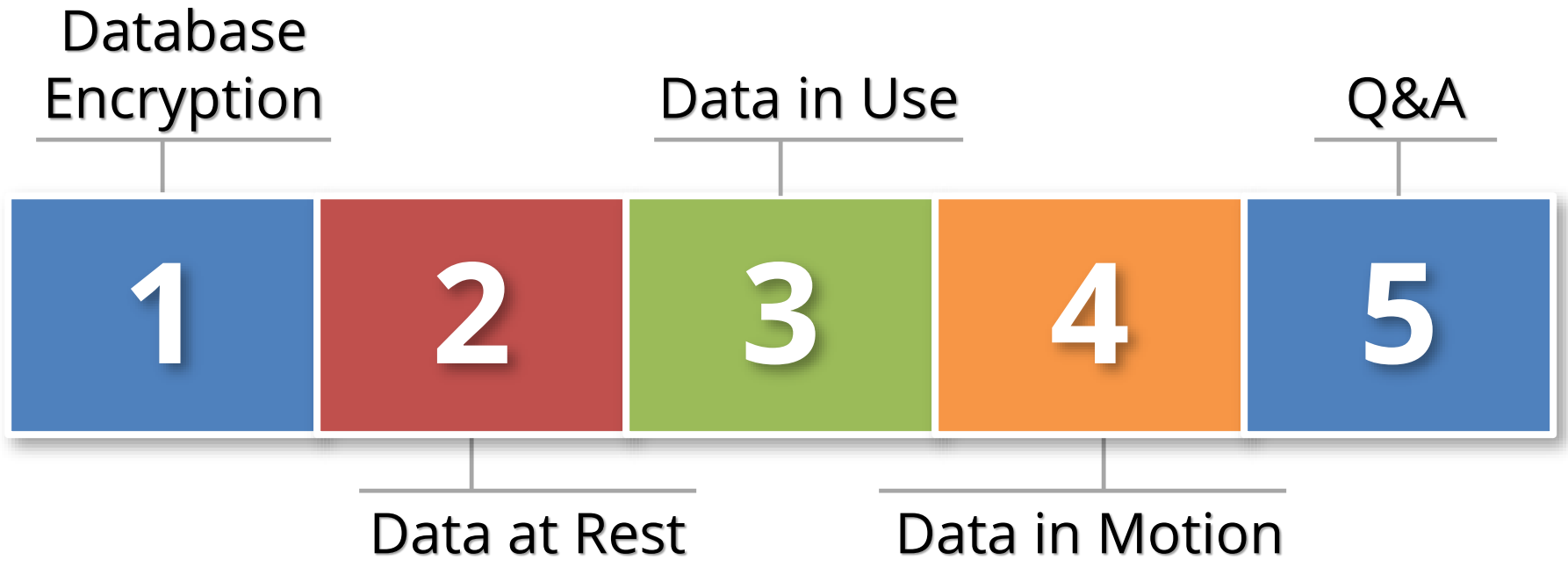
All Things Oracle Database Encryption

January 21, 2016

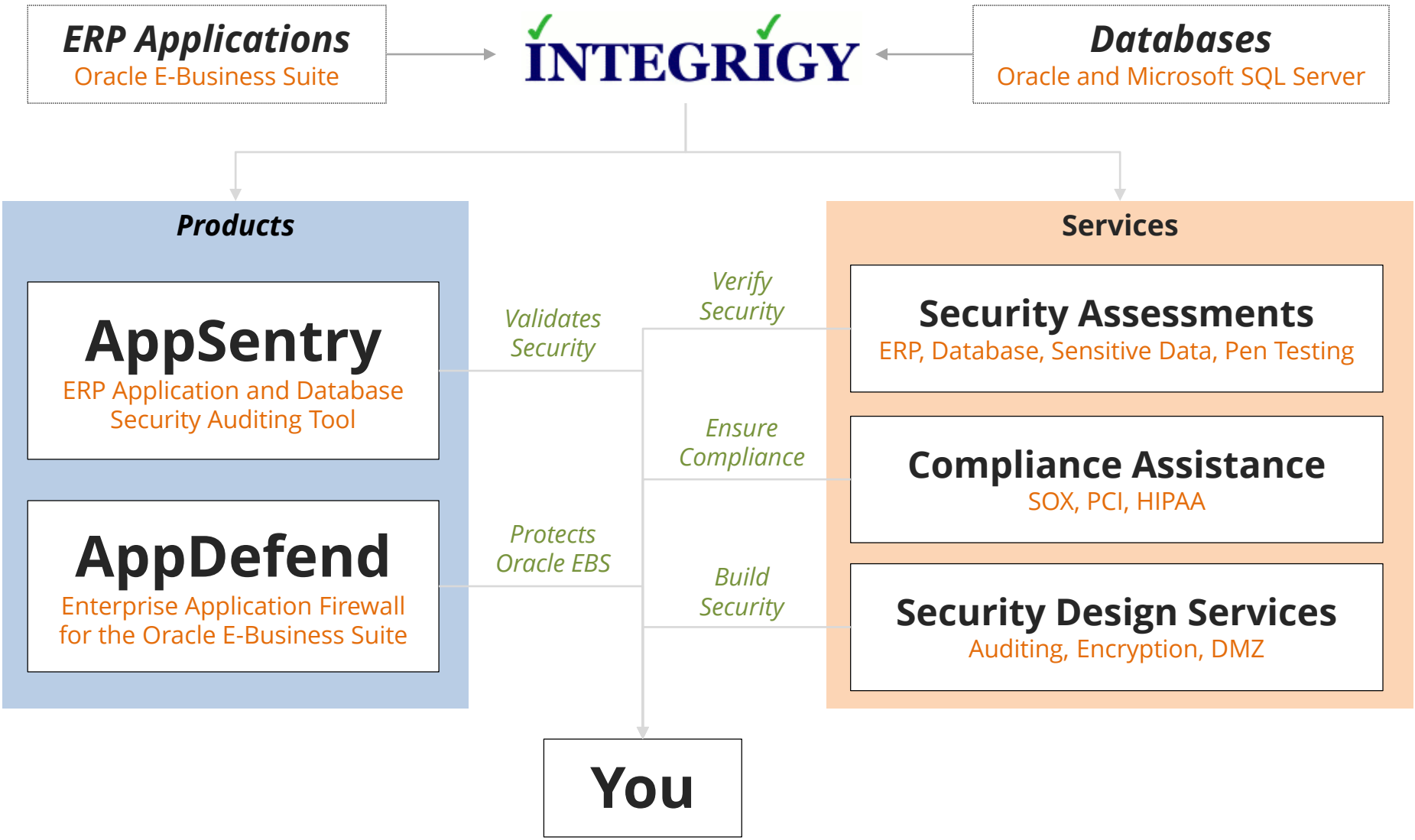
Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

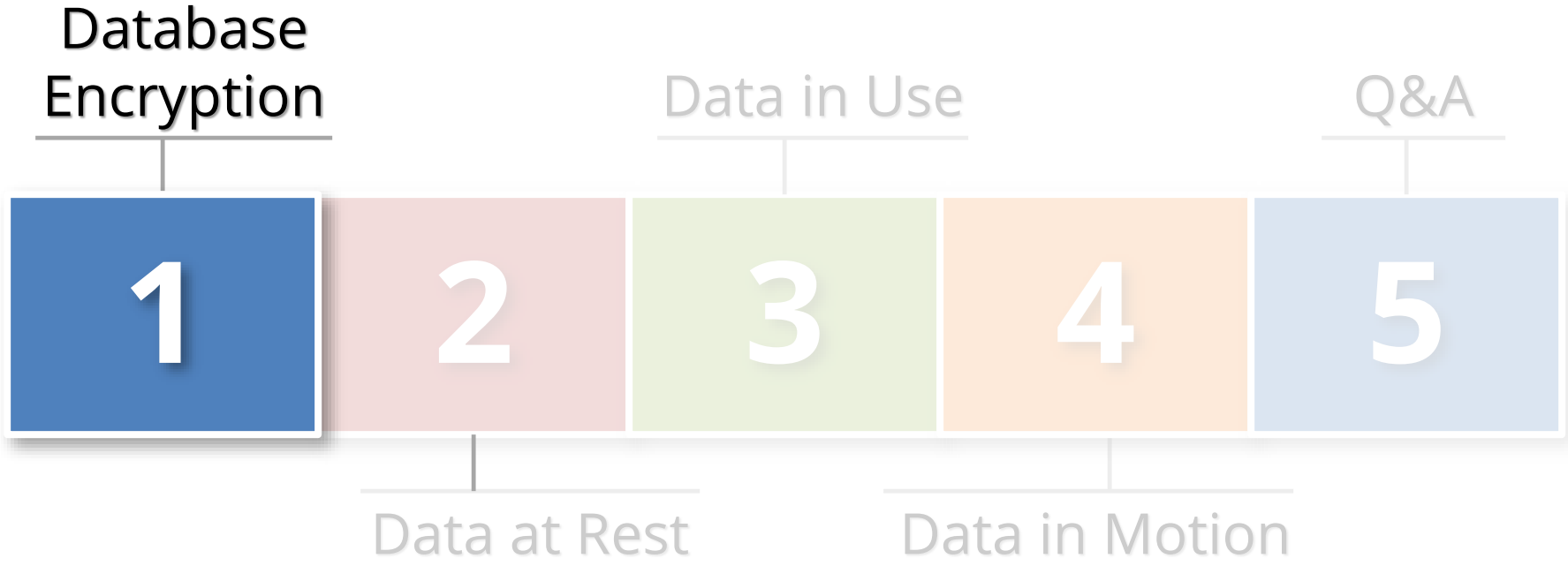
Agenda


Database Encryption
Data in Use
Q&A
1
2
3
4
5
Data at Rest
Data in Motion

About Integrigy



Agenda


Database Encryption
Data in Use
Q&A
1
2
3
4
5
Data at Rest
Data in Motion

What is Sensitive Data?

Payment Card Industry Data Security Standard (PCI-DSS 2.0)	▪ 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)

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

HIPAA Privacy Standard/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 Sensitive Data might be?

Application Tables

- Tables owned by the application and probably well-known

Custom tables

- Customizations to package applications 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 stored in temporary tables prior to processing

Database

Interface files

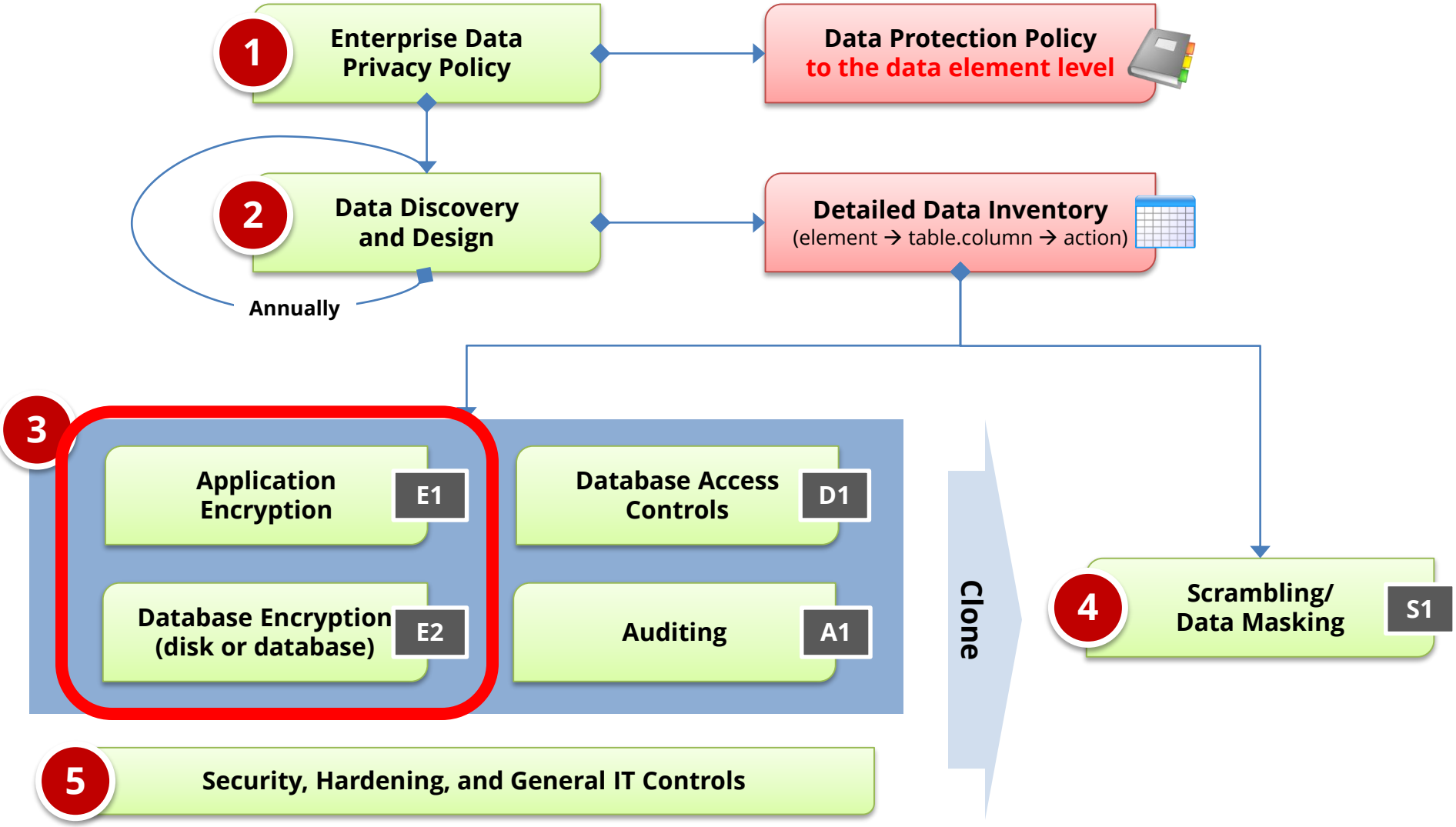
- Flat files used for interfaces or batch processing

Log files

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

File System

Integrigy Data Protection Process



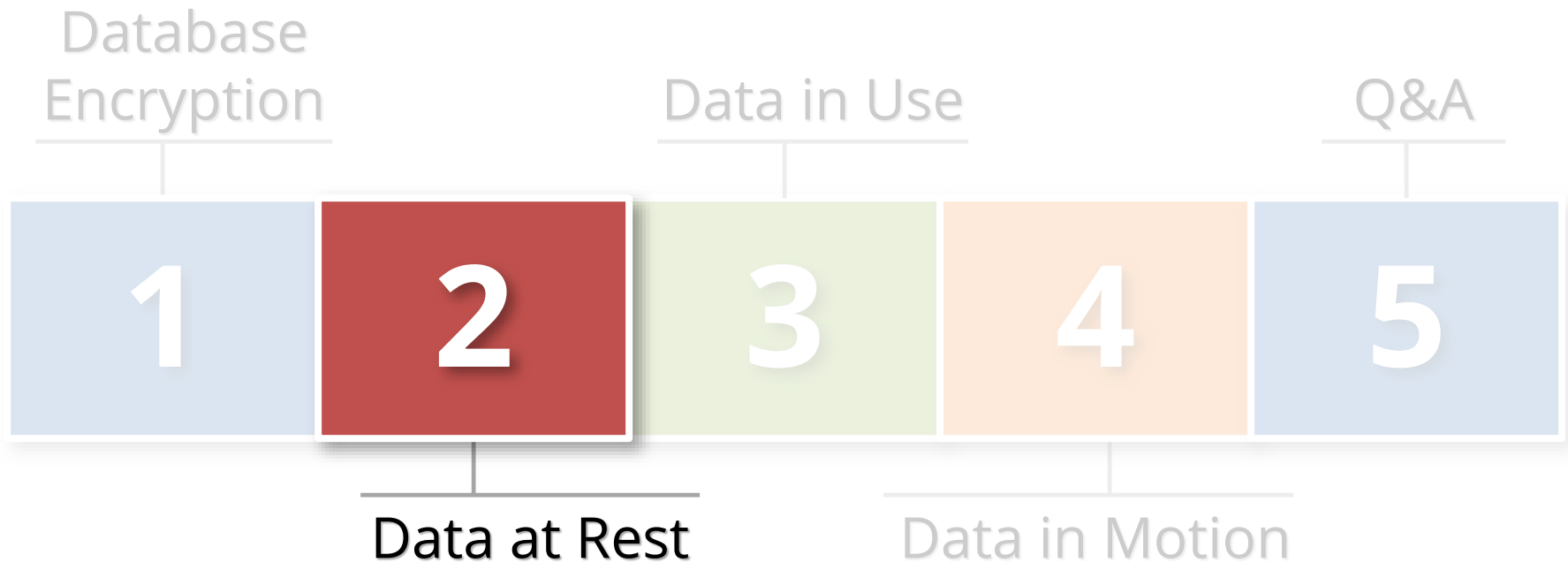
Types of Encryption

- **Storage (Data at rest)**
  - **Disk, storage, media level encryption**
  - Encryption of data at rest such as when stored in files or on media
- **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)

Storage/Access Oracle Encryption Solutions

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

Agenda


Database Encryption
Data in Use
Q&A
1
2
3
4
5
Data at Rest
Data in Motion

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

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**

Tablespace encryption

- Tablespace encryption only supported in 11g and 12c
- Tablespace must be exported and imported to implement encryption
- **Use for custom tablespaces or entire database**

Tablespace Encryption

- **Protects during operations like JOIN and SORT**
  - Data is safe when it is moved to temporary tablespaces
- **Allows index range scans on data in encrypted tablespaces**
  - Not possible with column-based transparent data encryption

Performance Considerations

- **Impact is limited to CPU performance**
  - Data must be encrypted and decrypted
  - Highly dependent on access patterns to data
  - Hardware cryptographic acceleration with AES-NI processors
- **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
  - 5% to 10% CPU performance impact for one customer on high transaction volume tables

Performance Considerations

1. **Range scan (between/like) on indexed column**
   - *where a.birth_date between start_date and end_date*
   - Index will not be used – full table scan
2. **Join on encrypted columns**
   - *where a.ssn = b.ssn*
   - Encryption key is unique for each table
   - Full table scan of both tables
   - All values in both tables decrypted

TDE Best Practices

- **Ensure wallet is not backed up with the db files**
- **Protect the wallet**
  - Backup the wallet
  - File permissions
- **When encrypting large volumes of data, should create a new tablespace and shred the old one**
  - Unencrypted data may remain in tablespace blocks
- **Mix and match column and tablespace encryption**
  - Column for standard tables and tablespace for custom
- **Avoid using PKI Certificates for master key**

Oracle TDE Demonstration

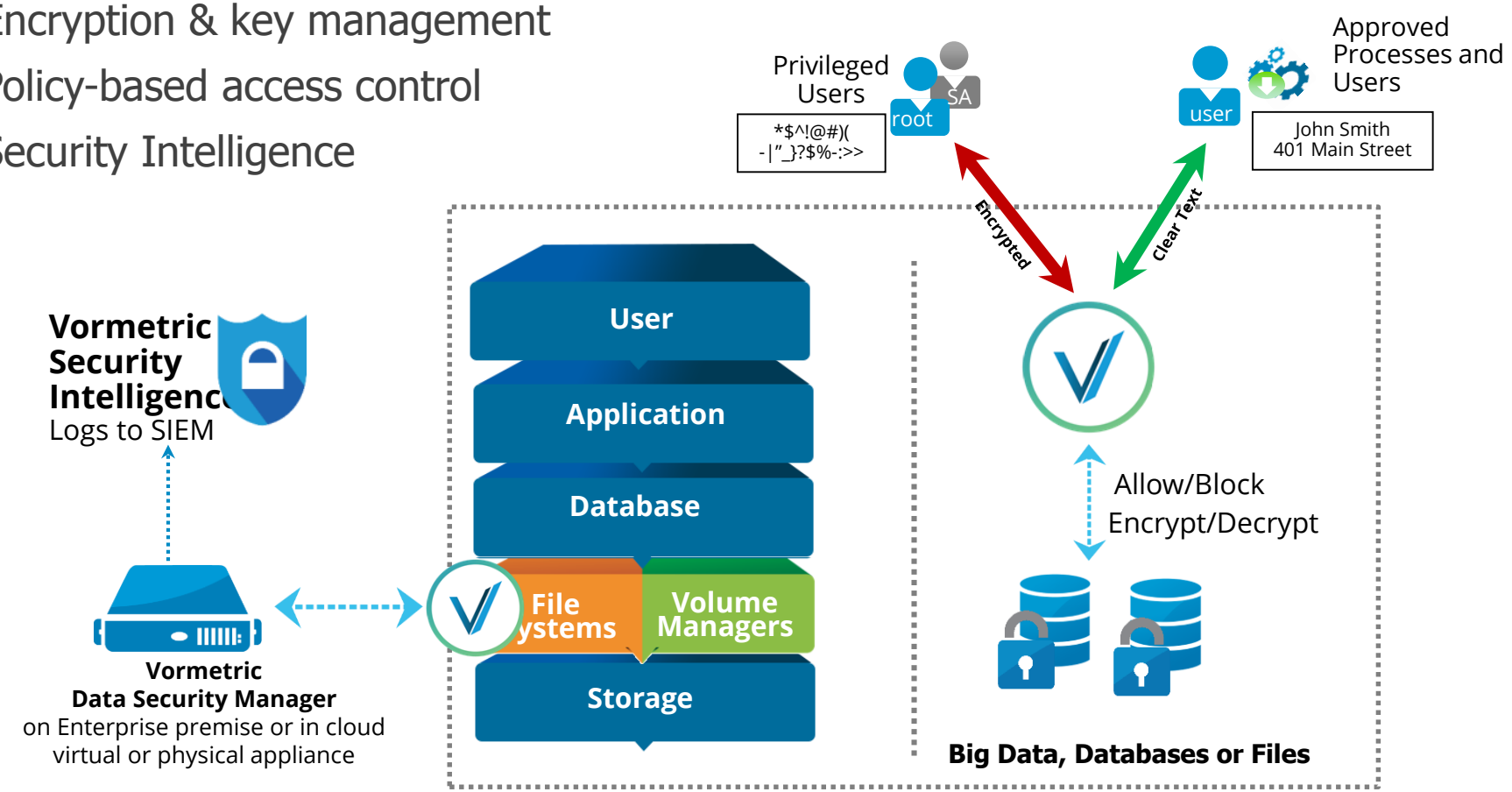
Hardware Security Modules (HSM)

- **HSMs are physical devices**
  - Secure storage for encryption keys
  - Secure computational space (memory) for encryption and decryption
- **Oracle TDE fully certified to use HSMs**
  - More secure alternative to the Oracle wallet
  - Several third party vendors
    - Vormetric

Third-Party Encryption - Vormetric

Vormetric Transparent Encryption

- Protects structured/unstructured data
- Encryption & key management
- Policy-based access control
- Security Intelligence



Auditing Oracle TDE Usage

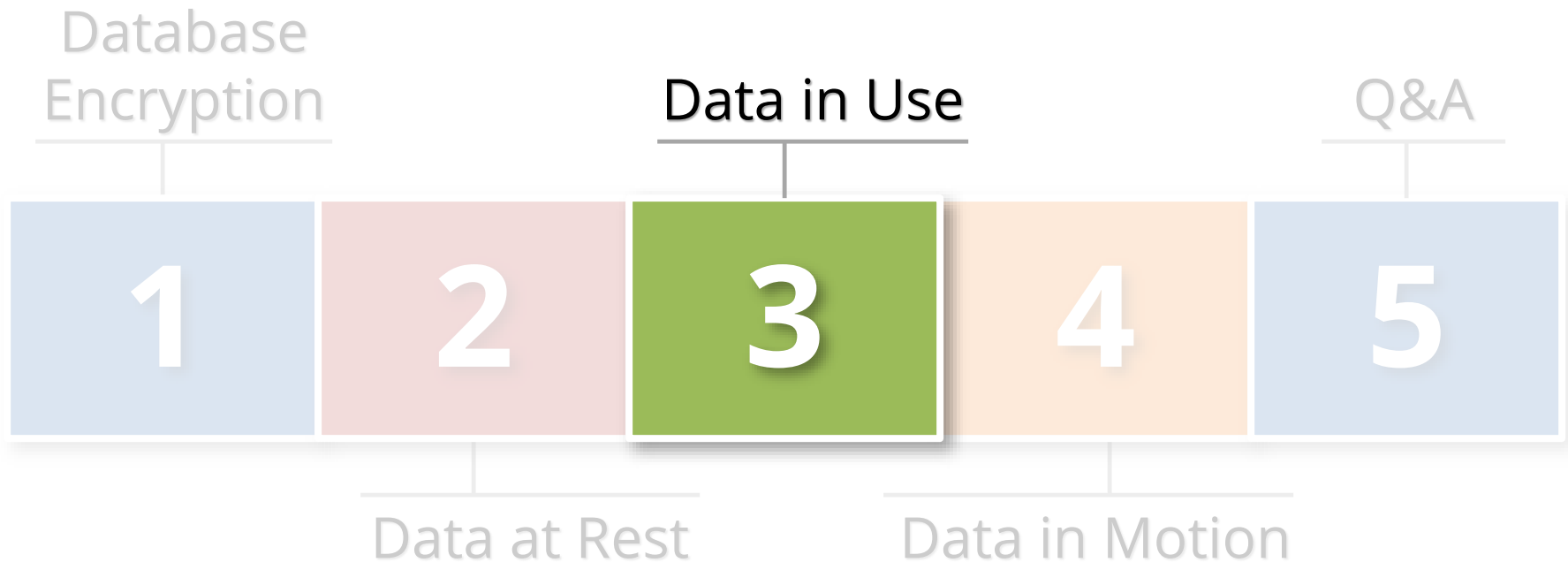
- **Key management is critical**
  - Where is wallet stored? Auto open? Backed up?
  - How is wallet protected? HSM used?

- **Column vs. Tablespace encryption**
  - What tables, columns, and tablespaces?
  - What Encryption algorithms?

```
SELECT * FROM dba_encrypted_columns;

SELECT tablespace_name, encrypted FROM dba_tablespaces;
```

Agenda


Database Encryption
Data in Use
Q&A
1
2
3
4
5
Data at Rest
Data in Motion

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

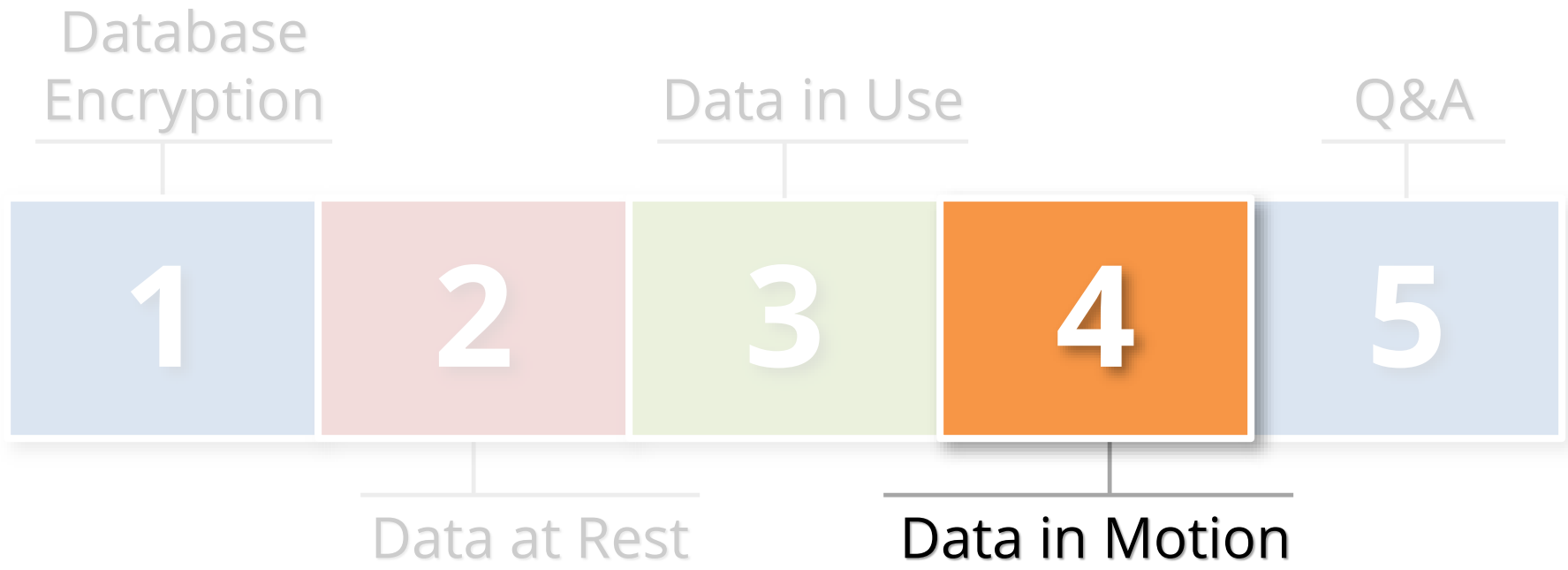
Oracle Database	▪ DBMS_CRYPTO
	  ▪ Supports most major encryption and hash algorithms
	  ▪ New database versions add newer encryption and hash algorithms
	  ▪ No key management
	▪ DBMS_OBFUSCATION_TOOLKIT
	  ▪ Deprecated and should not be used

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

Auditing Application Encryption

- **Difficult to audit as it is application specific and stored in application code**
  - Some package applications have robust encryption capabilities
- **Key management is critical**
  - How are keys stored, protected, rotated?
  - Keys should not be hard-coded in wrapped PL/SQL code – fairly common even for packaged applications
- **Methods and types of encryption**
  - What routines are used for encryption? Standard database, third-party libraries, custom developed?
  - Custom developed routines should never be used
  - What encryption algorithms are used?

Agenda


Database Encryption
Data in Use
Q&A
1
2
3
4
5
Data at Rest
Data in Motion

Database Network Encryption

- **Oracle SQL*Net Encryption**
  - Encrypts SQL*Net traffic between the client and the database listener
  - Configured in *sqlnet.ora*
  - Now included with the database – used to be part of Advanced Security Options (ASO)

- **All data will be encrypted transmitted between client and server**
  - The database password is always protected and never sent in clear-text

SQL*Net Encryption Setup

- Configure in *sqlnet.ora* on either or both the server and client
- Server

```
SQLNET.ENCRYPTION_SERVER = [accepted | rejected | requested
| required]
SQLNET.ENCRYPTION_TYPES_SERVER = (encryption algorithms)
```

- Client

```
SQLNET.ENCRYPTION_CLIENT = [accepted | rejected | requested
| required]
SQLNET.ENCRYPTION_TYPES_CLIENT = (encryption algorithms)
```

- *Algorithms =* **AES256 AES192 AES128 3DES168 3DES112** RC4_256 RC4_128 RC4_56 RC4_40 DES DES40

SQL*Net Encryption Options

		SERVER			
		Required	**Requested**	**Accepted**	**Rejected**
Client	**Required**	On	On	On	ERROR
	Requested	On	On	On	Off
	Accepted	On	On	Off	Off
	Rejected	ERROR	Off	Off	Off

Auditing SQL*Net Encryption

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

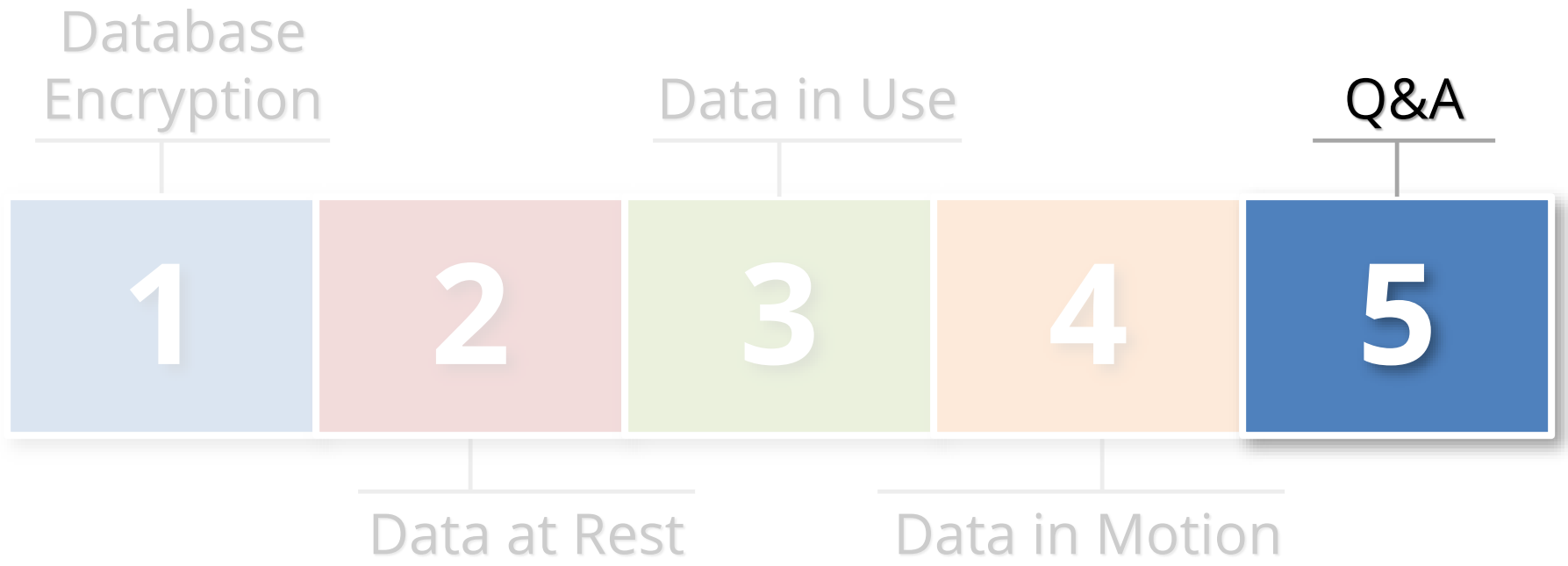
```
select NETWORK_SERVICE_BANNER
from v$session_connect_info
```

```
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
```

Auditing SQL*Net Encryption

- **Review the settings in sqlnet.net**
  - If encryption is required, then REQUIRED should be used
  - Review the encryption algorithms used – should be always AES and 3DES
- **Encryption and auditing**
  - If database auditing solutions such as Imperva or Guardium are used in network tap mode, then encryption may blind these tools

Agenda


Database Encryption
Data in Use
Q&A
1
2
3
4
5
Data at Rest
Data in Motion

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**