TOKENEX

The New York Oracle Users Group
Fall General Meeting – October 4, 2018

Next Generation Data Protection and Security for Oracle users – the Block Chain Advantage

Ulf Mattsson

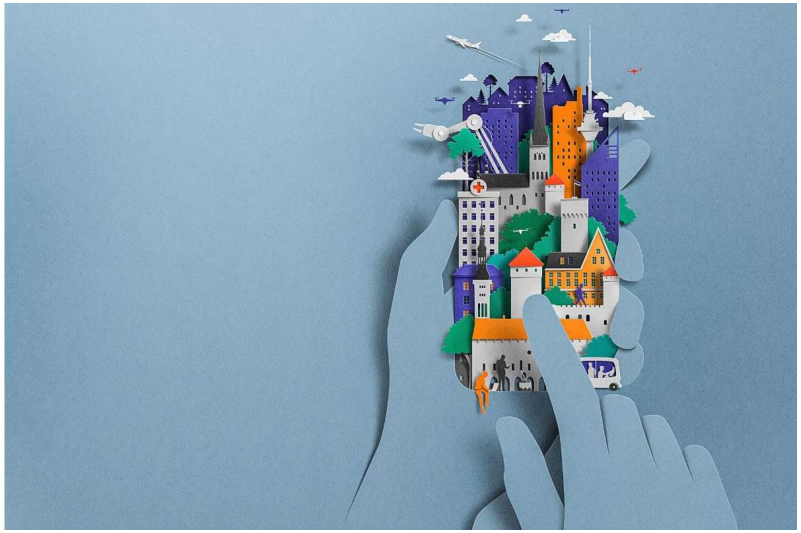
umattsson@tokenex.com

Phone: 203.570.6919

LETTER FROM TALLINN DECEMBER 18 & 25, 2017 ISSUE

ESTONIA, THE DIGITAL REPUBLIC

Its government is virtual, borderless, blockchained, and secure. Has this tiny post-Soviet nation found the way of the future?



The Netherlands National Blockchain Agenda

TOKENEX

Netherlands Delivers National Blockchain Agenda to Stimulate Research

By **David Bentley** - May 9, 2018 367

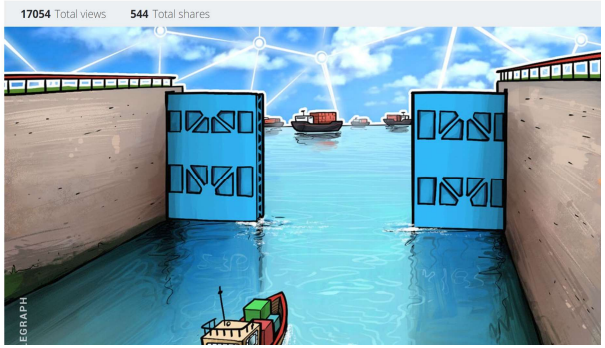
The Netherlands has announced its first National Blockchain Agenda, which will deliver several millions of euros for scientific research into the technology.

According to a press release Tuesday, the agenda was drawn up in partnership between government, knowledge institutions and the business community.

Presented to Rob van Gijzel, ambassador of the Dutch Blockchain Coalition, the agenda includes all areas relevant to further development of the blockchain, including technology, legal issues, economic impact and ethics. Both fundamental and applied research questions were incorporated. Multiple organizations will shape the agenda, through which several million euros will eventually become available for scientific research, according to the statement.

Source: David Bentley

Denmark Joins EU Blockchain Partnership, Plans to Implement Tech in Shipping



Denmark has signed a declaration to join a total of 24 European Union member states that support pan-EU blockchain standards and solutions, local news outlet Finans Watch reported June 4.

The EU blockchain partnership was formed on April 10 as part of the European Commission's Digital Day with the intention of enhancing cooperation among member states for developing blockchain tech.

Brian Mikkelsen, the Danish Minister for Industry, Business and Financial Affairs, said after signing the declaration Monday that Denmark will be "the first country in the world [to] use blockchain technology to register ships in the Danish ship registers." He added:

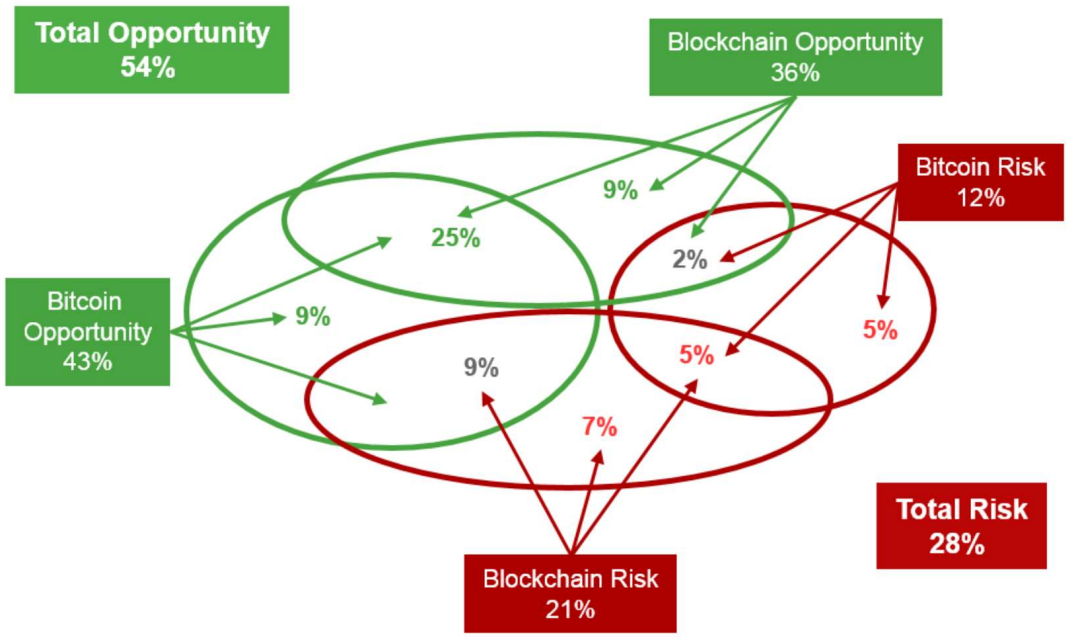
> *"Blockchain goes across borders, and a joint European cooperation is crucial to ensure future-proof standards and solutions. So I'm very pleased that we have now signed this declaration."*

Source: Danish Minister for Industry

Blockchain Board-Level Opinions

TOKENEX

Figure 2. Board-Level Opinions on Blockchain and Digital Currencies



Question: To what extent are bitcoin and blockchain a risk or an opportunity to your organization? (Percentage of respondents). Base = 100.

© 2017 Gartner, Inc.

Source: Gartner

Blockchain SWOT

TOKENEX

Figure 3. Blockchain Strengths, Weaknesses, Opportunities and Threats (SWOT)

Strengths	Weaknesses
▪ Distributed resilience and control ▪ Decentralized network ▪ Open source ▪ Security and modern cryptography ▪ Asset provenance ▪ Native asset creation ▪ Dynamic and fluid value exchange	▪ Lack of ledger interoperability ▪ Customer unfamiliarity and poor user experience ▪ Lack of intraledger and interledger governance ▪ Lack of hardened/tested technology ▪ Limitation of smart contract code programming model ▪ Wallet and key management ▪ Poor tooling and poor developer user experience ▪ Skills scarcity and cost ▪ Immature scalability ▪ Lack of trust in new technology suppliers
Opportunities	**Threats**
▪ Reduced transaction costs ▪ Business process acceleration and efficiency ▪ Reduced fraud ▪ Reduced systemic risk ▪ Monetary democratization ▪ New business-model enablement ▪ Application rationalization and redundancy	▪ Legal jurisdictional barriers ▪ Politics and hostile nation-state actors ▪ Technology failures ▪ Institutional adoption barriers ▪ Divergent blockchains ▪ Ledger conflicts/competition ▪ Poor governance

© 2017 Gartner, Inc.

Source: Garter

Blockchain in Healthcare

TOKENEX

THE WALL STREET JOURNAL.

ne World U.S. Politics Economy **Business** Tech Markets Opinion

Five Possible Uses for Blockchain in Health Care

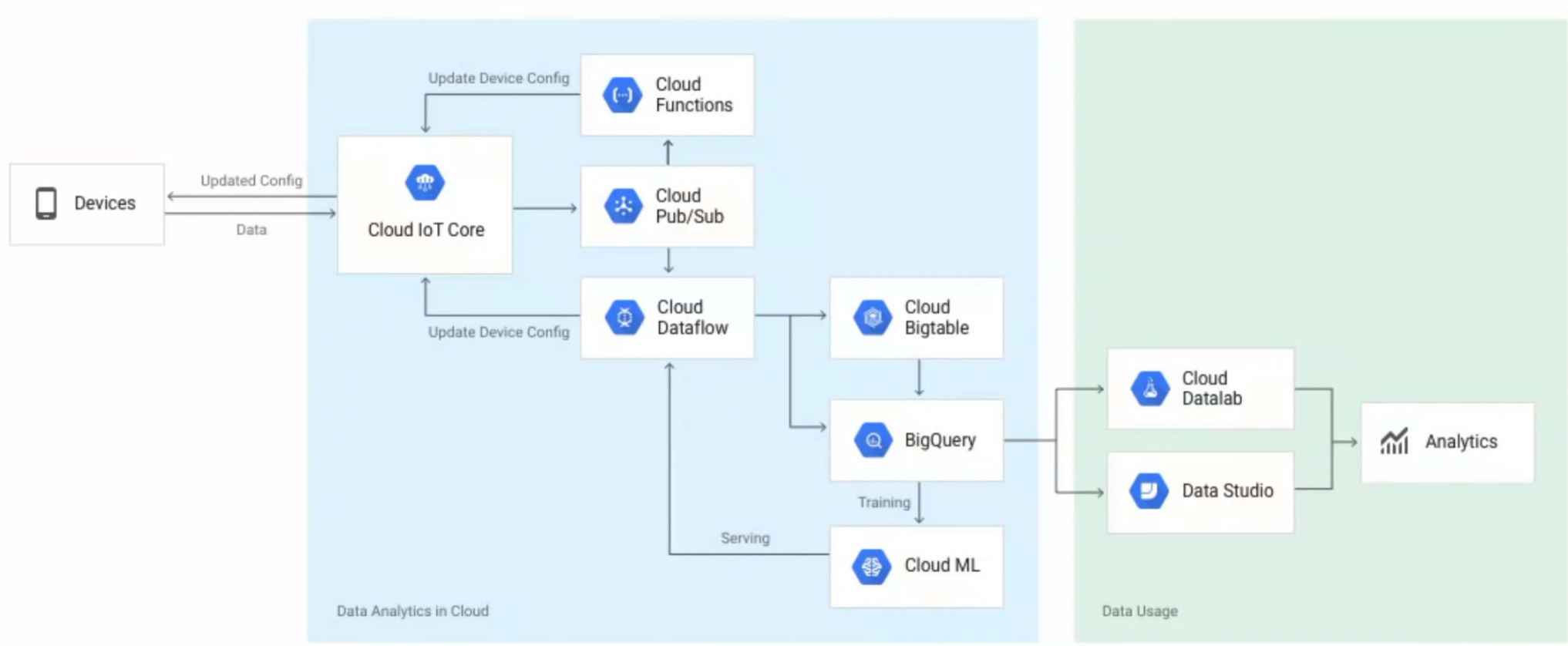
Greg Reh

When I bring up blockchain in client meetings, or in dinner conversations, people tend to have one of two reactions. Either they see it as being synonymous with bitcoin and other digital currencies, or they see blockchain as an overhyped technology.

I agree there is a lot of hype swirling around blockchain, and I also agree that this technology likely isn't going to turn health care on its head. We might still be five or 10 years from realizing the potential of blockchain. But I do think it could help life

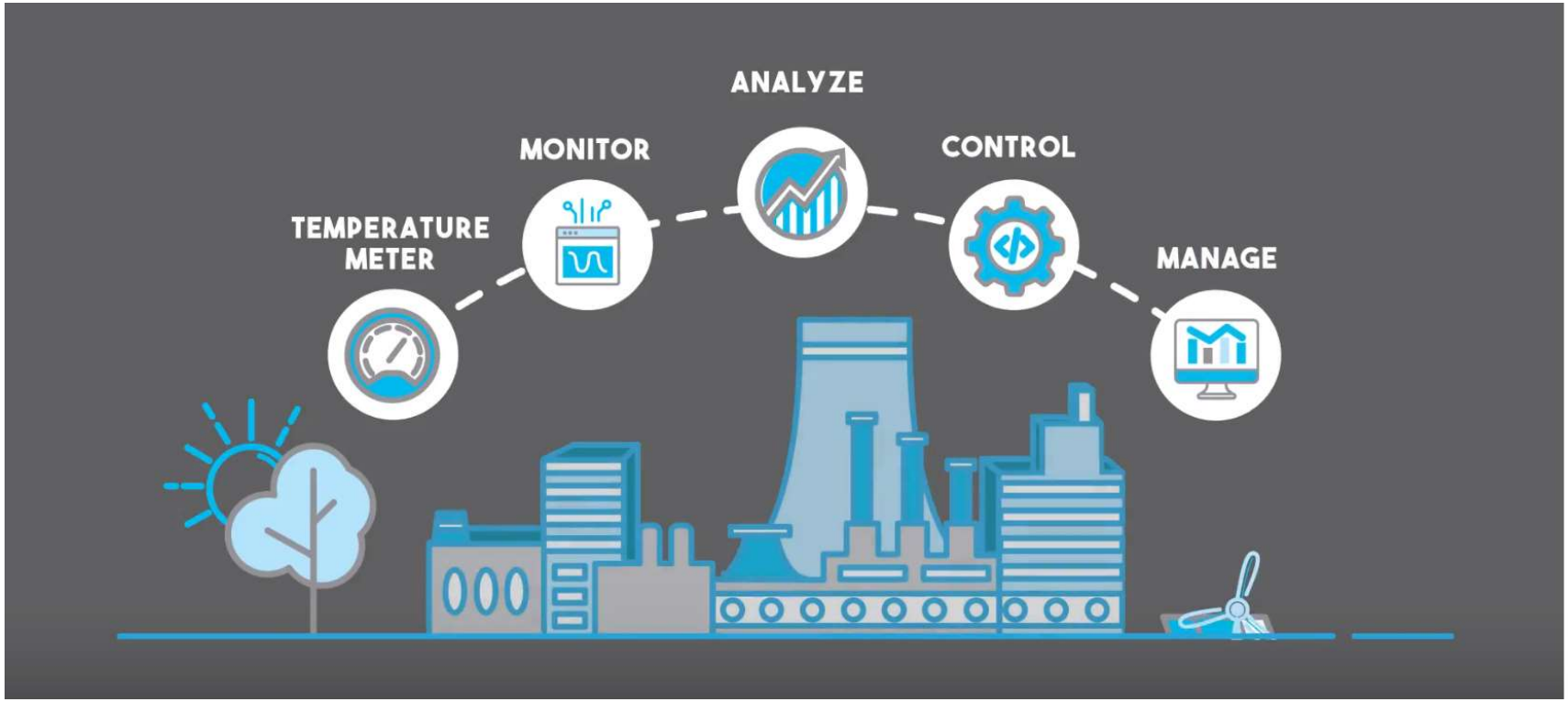
Source: THE WALL STREET JOURNAL

IoT Data Flow

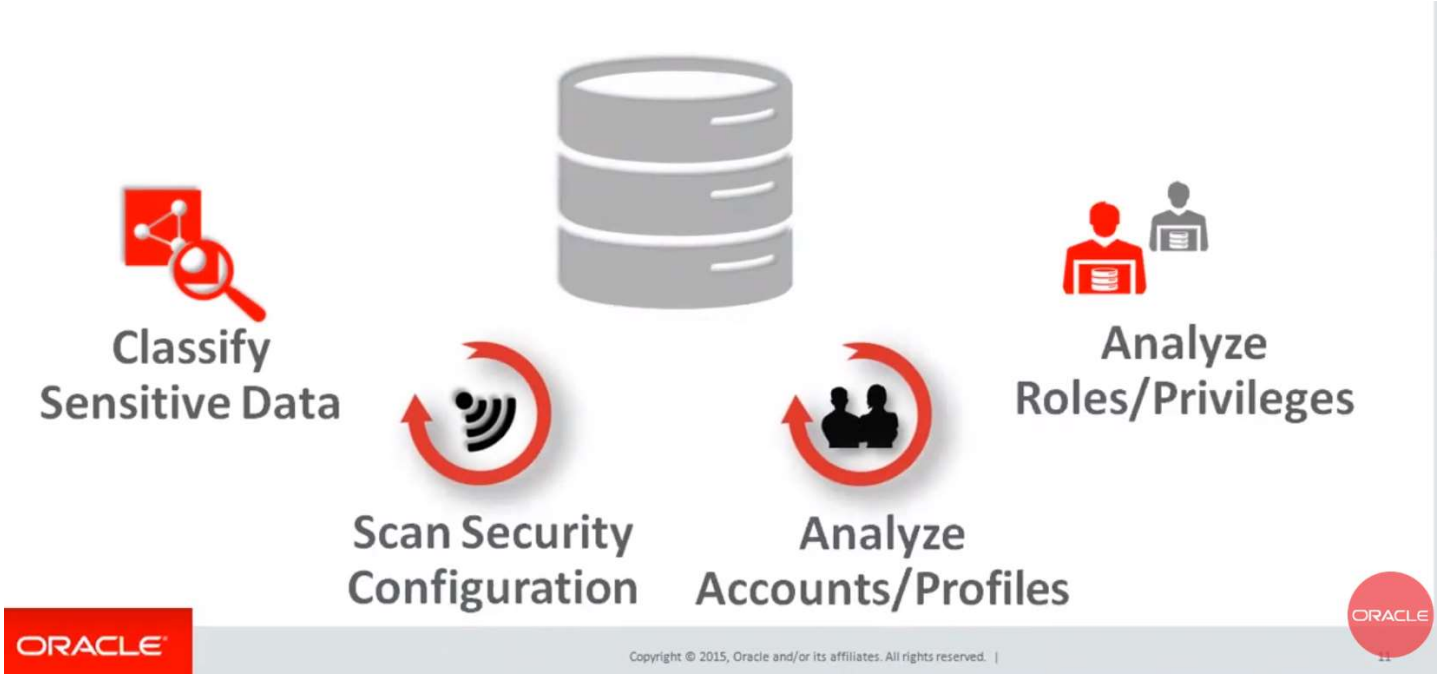


Source:iot-core

IoT-Enabled Energy Management Solutions are Game-Changers



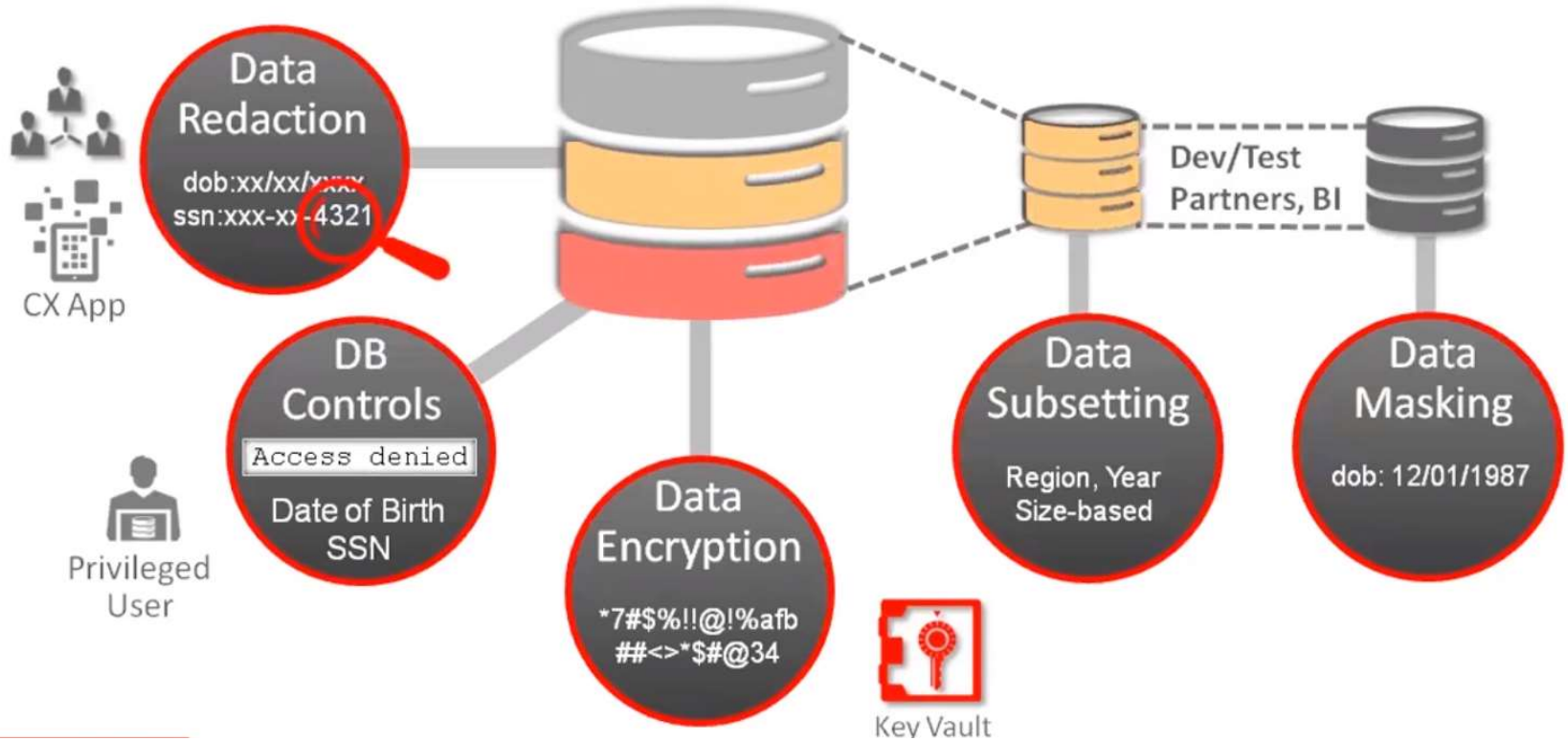
Evaluate Security Risk



Source: Oracle

Protect Databases from Attacks

TOKENEX



Source: Oracle

European Union GDPR Aim

TOKENEX

Data Protection and Privacy

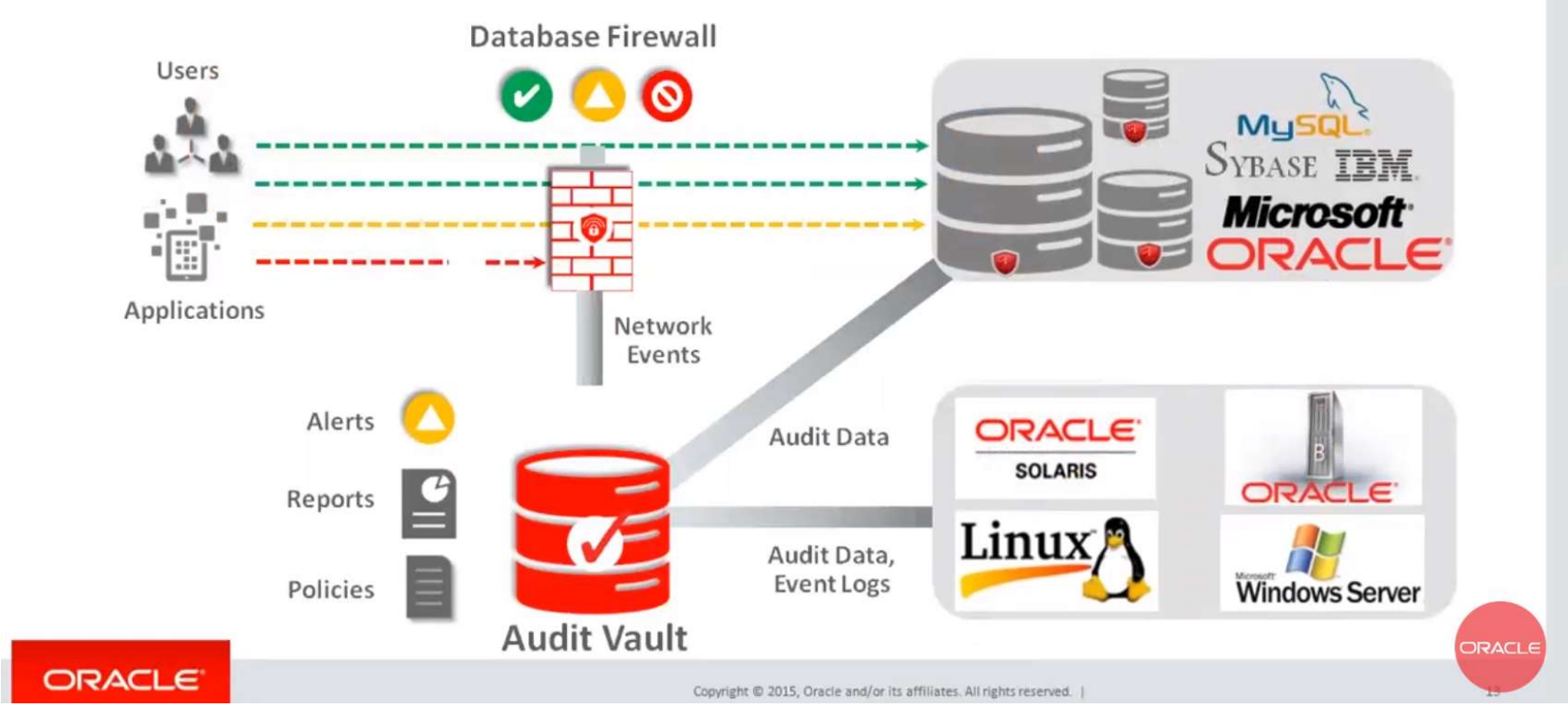
Unify Data Protection within the EU with a single law

- **Regulation** not a Directive **Does not require any enabling legislation** to be passed by governments
- Immediate effect on 28 EU members after **2 year transition period**
- **Extends the scope to all foreign companies** processing data of EU residents

Source: Oracle

Audit, Monitor and Detect

TOKENEX



Source: Oracle

Defense-in-Depth Security Controls

TOKENEX

EVALUATE	PROTECT	DETECT
Security Configuration	Encryption & Redaction	Auditing
Sensitive Data Discovery	Masking & Subsetting	Activity Monitoring
Least Privilege Use	DBA & Operational Controls	Alerting & Reporting

ORACLE

ORACLE

ORACLE

ORACLE

Copyright © 2015, Oracle and/or its affiliates. All rights reserved. |

Source: Oracle

Oracle Database Security Strategy

TOKENEX

Adressing the EU GDPR from the Inside Out

SECURITY INSIDE OUT

Effective Security is close to the data.
Maximize performance with application transparency.

DEFENSE IN DEPTH

Layered overlapping controls: Encryption, audit, monitoring, access control, masking, redaction, …

SECURE DEPLOYMENTS

Across multiple systems: operating systems, heterogeneous databases, applications, big data, …

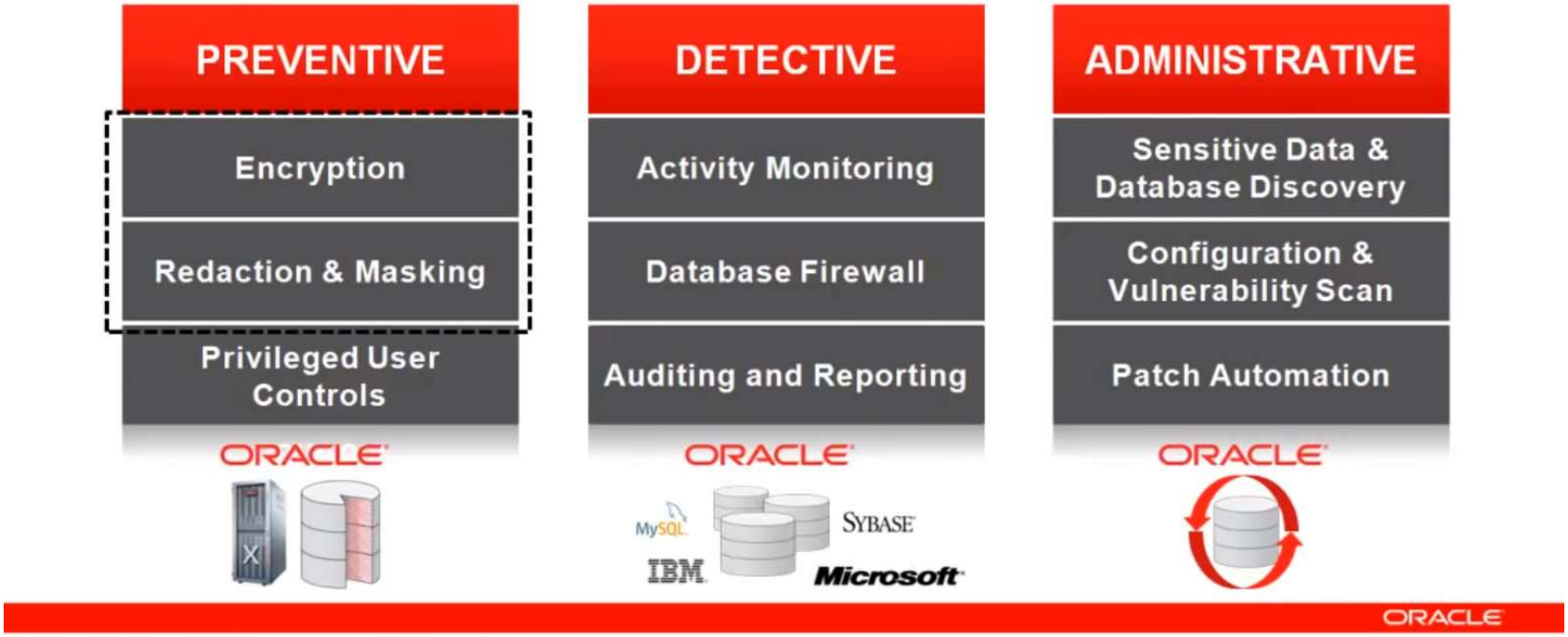
CONTINUOUS INNOVATIONS

VPD, TDE, DBA Control, Redaction, Privilege Analysis, Database Firewall, Real Application Security, ….

Source: Oracle

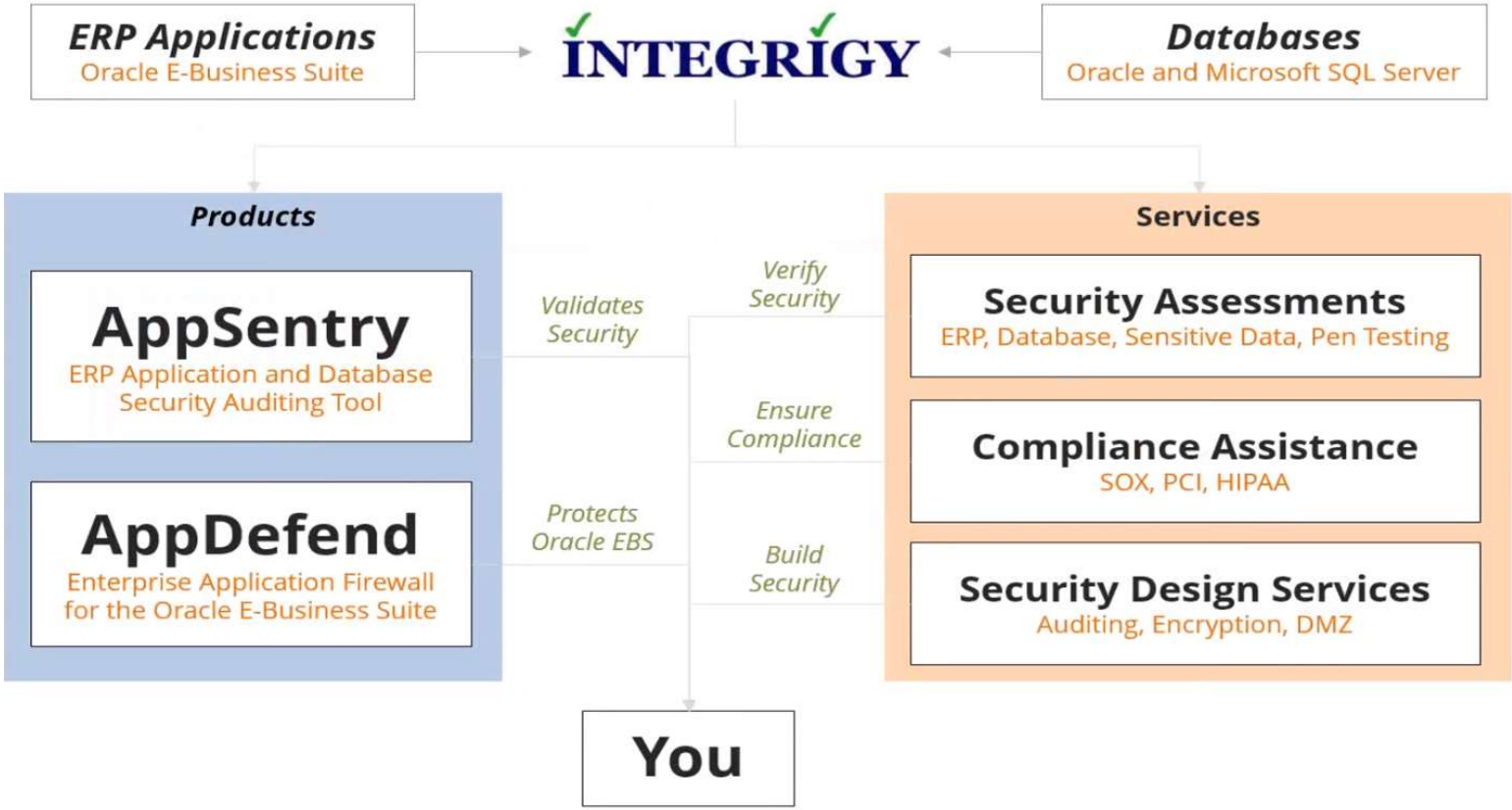
Oracle Database Security

TOKENEX



Source: Oracle

About Integrigy Corp



Source: Integrigy Corporation

Where Sensitive Data might be

TOKENEX

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

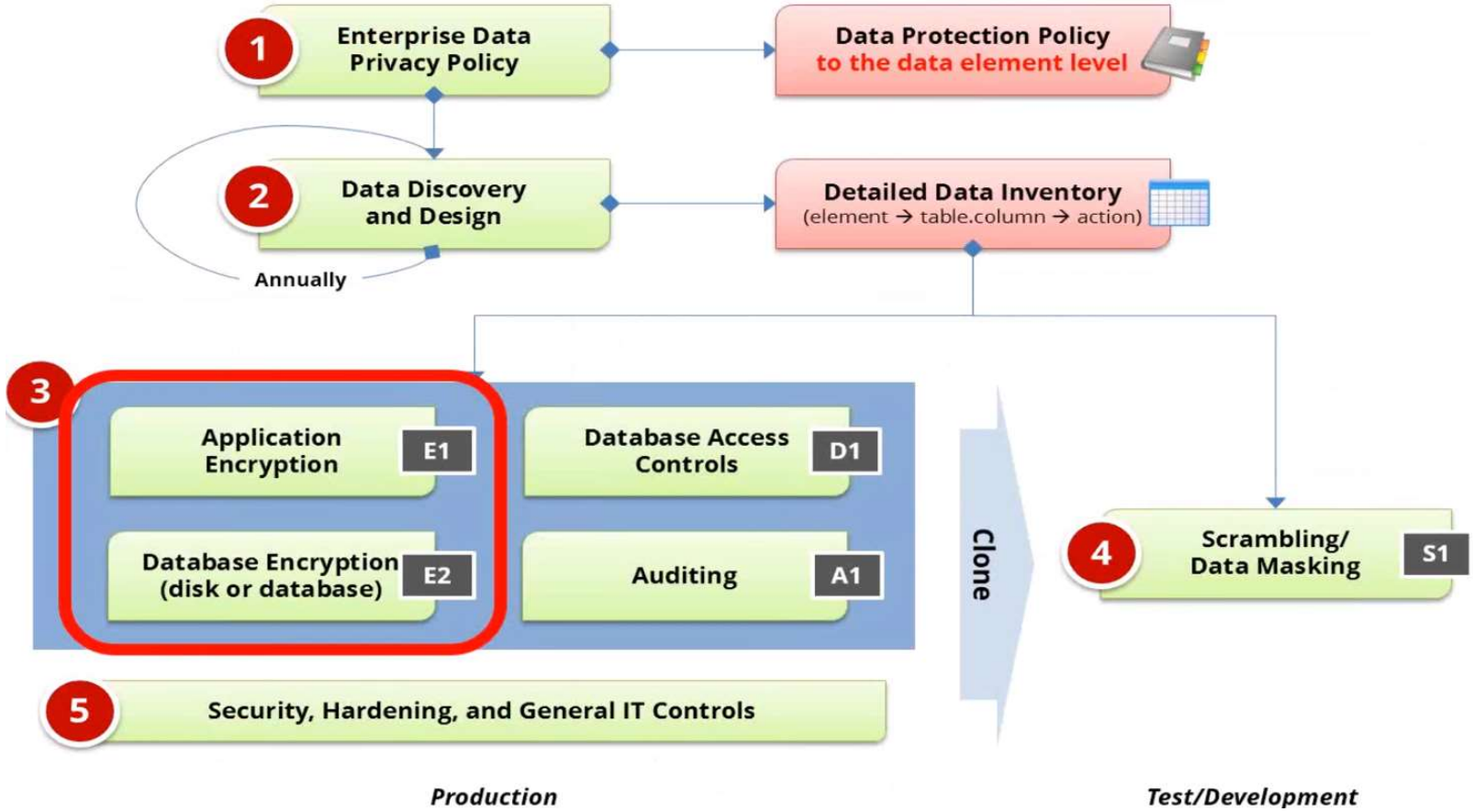
- Log files generated by the application (e.g., iPayment)

File System

Source: Integrigy Corporation

Integrigy Data Protection Process

TOKENEX



Source: Integrigy Corporation

Types of Encryption

TOKENEX

- 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)

Source: Integrity

Types of Encryption

TOKENEX

- 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)

Source: Integrity

Storage/Access Oracle Encryption Solutions

TOKENEX

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**

Source: Integrity

What is Oracle TDE?

TOKENEX

- **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

Source: Integrity

Tablespace Encryption

TOKENEX

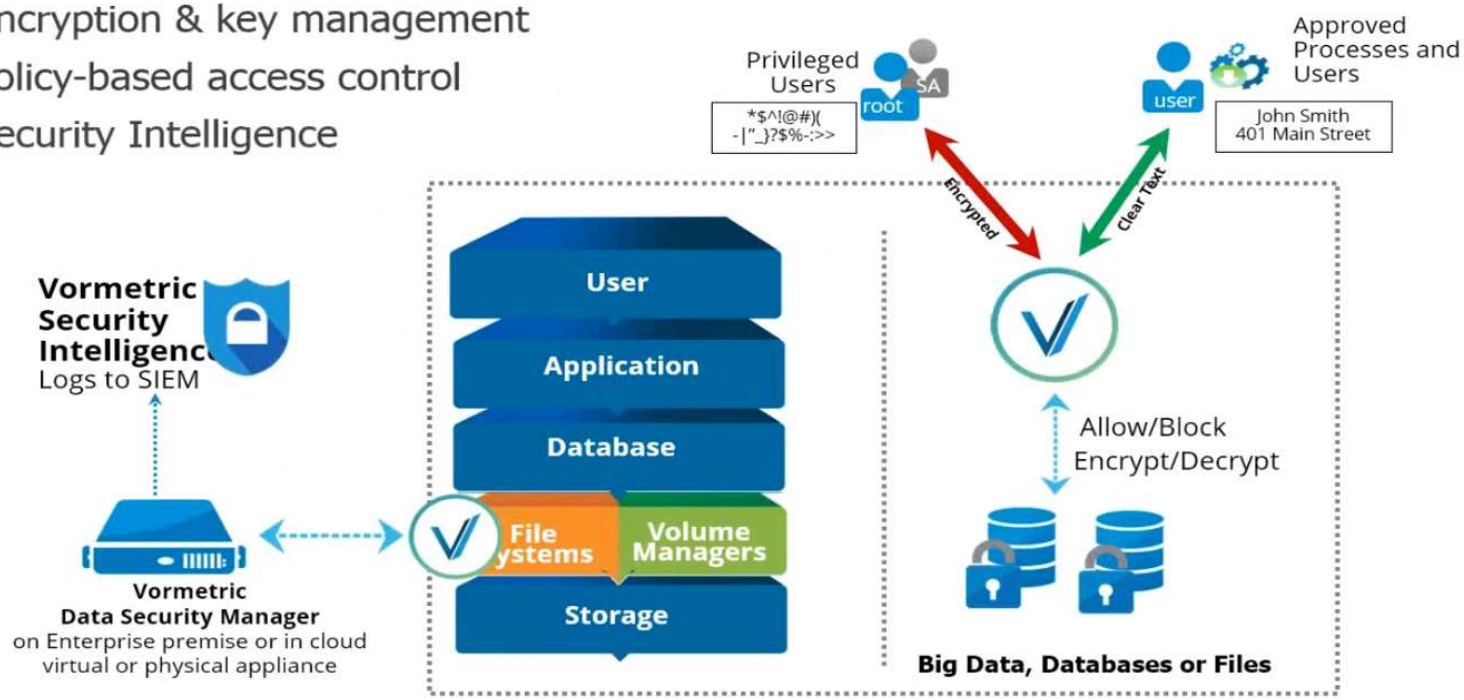
- **Protects during operations like JOIN and SORT**
  - Data is safe when it is moved to temporary tablespaces
- **Allows index range scans on data in encrypted tablespaces**
  - Not possible with column-based transparent data encryption

Source: Integrity

TOKENEX

Vormetric Transparent Encryption

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



GDPR MAIN BENEFITS

TOKENEX

- Right to be Forgotten, to Erasure and Rectification
- Easier Access to your own data
- Allowing you to decide how your data is used
- The right to know when your data has been hacked
- Data protection first, not an afterthought
- One-stop-shop
- European regulators will be equipped with strong enforcement powers
- One continent, one law

Source: Oracle

GDPR FINES

TOKENEX

Administrative Fines

The supervisory authority may impose fines…

Fine	Reason
Up to **250 000 EUR**, or in case of an undertaking 0,5 % of its total worldwide annual turnover	(a)Does not respond within the period referred to in Article 12(2) to requests of the data subject; (b) charges a fee in violation of the first sentence of paragraph 4 of Article 12.
Up to **500 000 EUR**, or in case of an undertaking 1% of its total worldwide annual turnover	(a) does not provide the information, or (…) provides incomplete information, or does not provide the information [timely or] in a [sufficiently] transparent manner, to the data subject pursuant to Articles 12(3),14 and 14a; (b) does not provide access for the data subject or does not rectify personal data pursuant to Articles 15 and 16 (…); (c) does not erase personal data in violation of the right to erasure and 'to be forgotten' …

ORACLE

Copyright © 2015 Oracle and/or its affiliates. All rights reserved.

ORACLE

Source: Oracle

A GDPR FRAMEWORK - 5 KEY ACTIVITIES TO ADDRESS GDPR

TOKENEX

Security requirements	Assess	Design	Transform	Operate	Conform
	PREPARE: • Assess security current state, identify gaps, benchmark maturity, establish conformance roadmaps • Identify vulnerabilities, supporting Security by Design **DISCOVER:** • Discover and classify personal data assets and affected systems to design security controls	**ROADMAP:** • Create security remediation and implementation plan **SECURITY BY DESIGN:** • Create security reference architecture • Design Technical and Organizational Measures (TOMs) appropriate to risk (such as encryption, pseudonimization, access control, monitoring)	**PROTECT:** • Implement privacy-enhancing controls (for example, encryption, tokenization, dynamic masking) • Implement security controls; mitigate access risks and security vulnerabilities	**MANAGE SECURITY PROGRAM:** • Manage and implement security program practices such as risk assessment, roles and responsibilities, program effectiveness **RUN SERVICES:** • Monitor security operations and intelligence: monitor, detect, respond to and mitigate threats • Govern data incident response and forensics practices	**DEMONSTRATE:** • Demonstrate technical and organizational measures to ensure security appropriate to processing risk • Document security program: ongoing monitoring, assessment, evaluation and reporting of security controls and activities **RESPOND:** • Respond to and manage breaches

Discover Data Assets

Security by Design

Encryption and Tokenization

Source: GDRP framework

KEY ACTIVITIES TO ADDRESS GDPR – TokenEx Example

TOKENEX

GDPR and TokenEx

GDPR Article 6(4)e):

"Encryption"

TokenEx:

"Tokenization"

If you are a data controller who has a valid reason--other than consent from the data subject--for the processing of his or her personal data "for a purpose other than that for which the personal data have been collected", Article 6(4)(e) obligates you to use "appropriate safeguards, which may include encryption or pseudonymization.

The TokenEx platform enables you to pseudonymize personal data within your environment, by replacing it with tokens, and storing the personal data in an encrypted TokenEx cloud token vault.

GDPR Article 25(1):

"Data Protection by Design" Article 25(1): "Encryption"

TokenEx:

"Tokenization and Encryption"

The GDPR requires "data protection by design and by default." Article 25(1) specifically obligates controllers to "…implement appropriate technical and organizational measures, such as pseudonymization."

The TokenEx platform enables you to pseudonymize personal data within your environment, replacing it with tokens, and storing the data in an encrypted TokenEx cloud token vault. The pseudonymized data will likely present a lower risk, thus possibly reducing the number of additional security measures required to meet this obligation. Using a cloud-based tokenization provider like TokenEx to pseudonymize direct identifiers in the personal data your controls is a clear indication that you are considering data protection by design and striving to implement technical measures appropriate to the risk.

GDPR Article 32(1)

"Pseudonymization of Personal Data"

TokenEx:

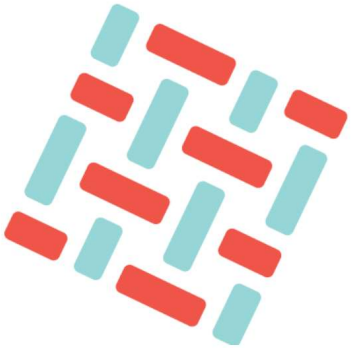
"Pseudonymize Personal Data"

Article 32(1) obligates controllers as well as processors to "implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk," including pseudonymization of personal data.
The TokenEx platform enables you to pseudonymize personal data within your environment, replacing it with tokens, and storing the data in an encrypted TokenEx cloud token vault. The pseudonymized data will likely present a lower risk, thus possibly reducing the number of additional security measures required to meet this obligation.

Source: https://tokenex.com/gdpr

Blockchain based on Open Source

TOKENEX



HYPERLEDGER FABRIC

Oracle Blockchain Cloud Service is based on the Open Source Hyperledger Fabric v1.0, so naturally the launch of Hyperledger v1.1 from the open source Hyperledger community is a welcome innovation for Oracle Blockchain Cloud Service and its customers.

Hyperledger Fabric is a blockchain framework implementation and one of the Hyperledger projects hosted by The Linux Foundation. Hyperledger Fabric allows components, such as consensus and membership services, to be plug-and-play. Hyperledger Fabric leverages container technology to host smart contracts called “chaincode” that comprise the application logic of the system.

Source: Oracle

BEST PRACTICE - FIND AND PROTECT YOUR SENSITIVE DATA

TOKENEX

Base:127 IT and security decision makers at organizations of 500 or more employees
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, August 2017

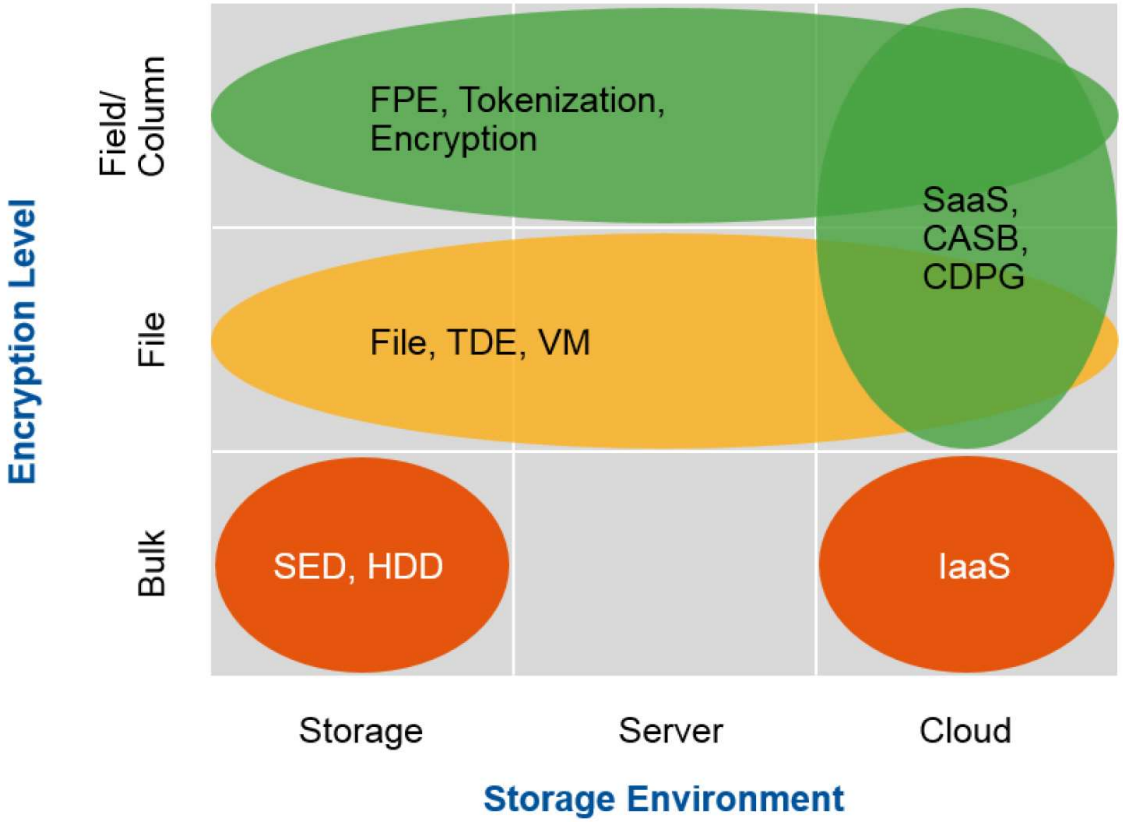
DATA DE-IDENTIFICATION / ANONYMIZATION

TOKENEX

Field	Real Data	Tokenized / Pseudonymized
Name	Joe Smith	csu wusoj
Address	100 Main Street, Pleasantville, CA	476 srta coetse, cysieondusbak, CA
Date of Birth	12/25/1966	01/02/1966
Telephone	760-278-3389	760-389-2289
E-Mail Address	joe.smith@surferdude.org	eoe.nwuer@beusorpdqo.org
SSN	076-39-2778	076-28-3390
CC Number	3678 2289 3907 3378	3846 2290 3371 3378
Business URL	www.surferdude.com	www.sheyinctao.com
Fingerprint		Encrypted
Photo		Encrypted
X-Ray		Encrypted
Healthcare / Financial Services	Dr. visits, prescriptions, hospital stays and discharges, clinical, billing, etc. Financial Services Consumer Products and activities	Protection methods can be equally applied to the actual data, but not needed with de-identification

Source: Customer Case Study

ENCRYPTION & TOKENIZATION LEVELS



FPE = format preserving encryption; HDD = hard-disk drive; CASB = cloud access security broker; CDPG = cloud data protection gateway; SED = self-encrypting drive; TDE = transparent data encryption.

Source: Gartner

ENCRYPTION AND TOKENIZATION BEST PRACTICES

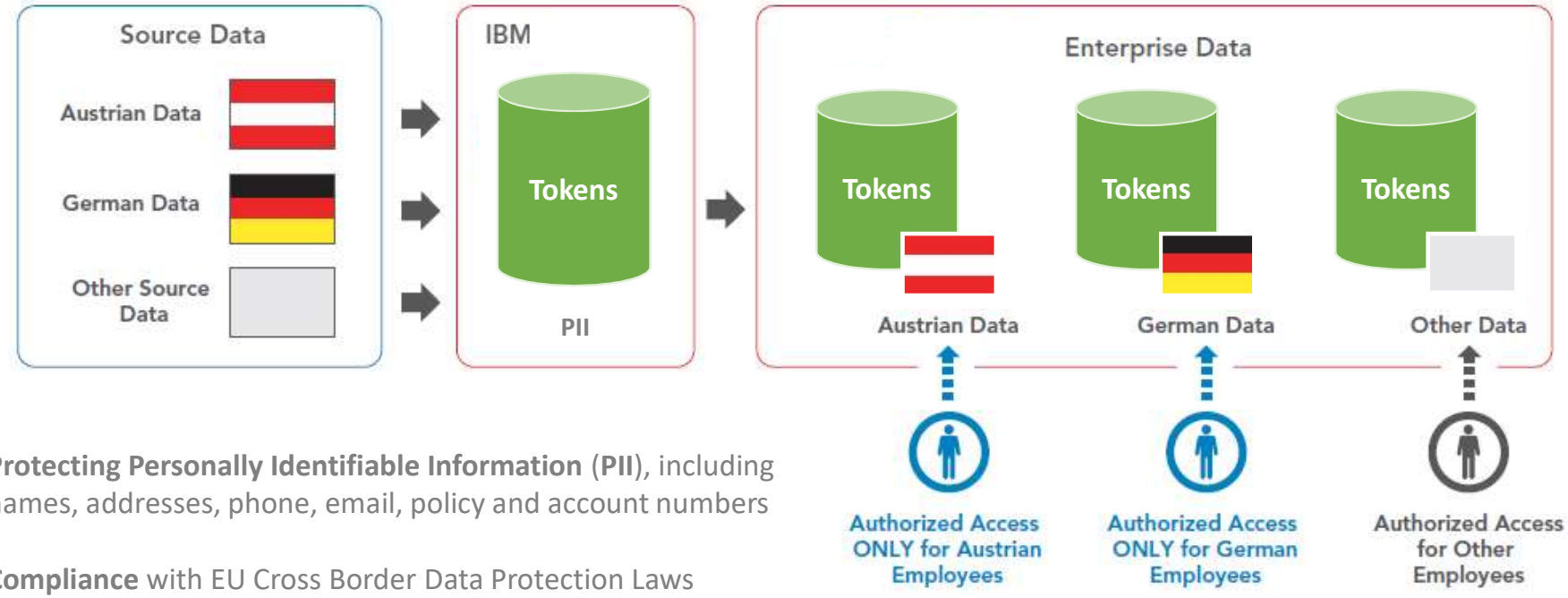
TOKENEX

Less Secure	**Storage Encryption** Pervasive protection of storage devices — storage area network/network-attached storage.	**Warnings** No access controls.
	File and Database Encryption Transparent to apps/database management system (DBMS). Prevents access to system administrators.	**Warnings** Authorized users and DBAs can still see clear text, plus developers/test engineers.
More Secure	**FPE/Tokenization** Transparent to apps/DBMS. Protects stored data and data in use. RBAC prevents DBA access.	**Warnings** All authorized users see clear text. Connection pooling may hide user identities = no RBAC.
	Application Encryption Strongest access controls.	**Warnings** App-specific integrations required — other apps will suffer any data changes.

Source: Gartner

PROTECT PII DATA CROSS BORDER - BEST PRACTICES

TOKENEX

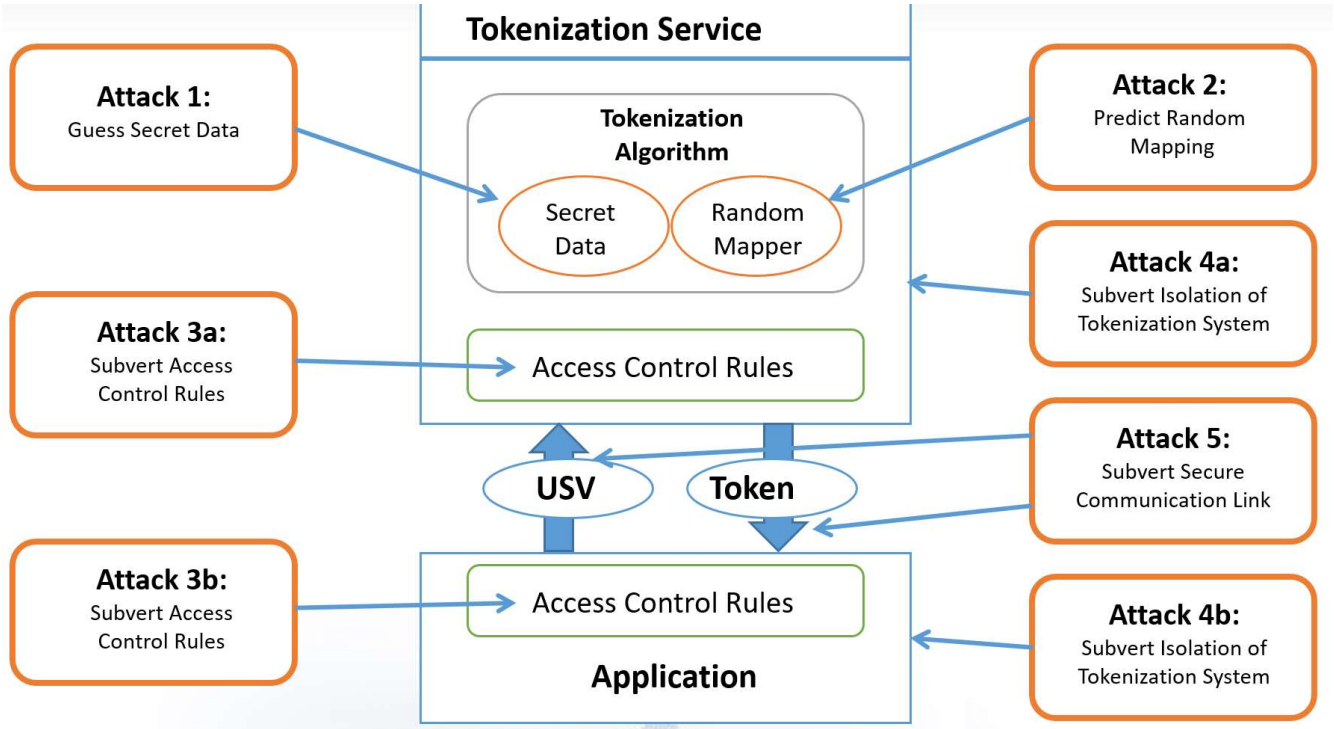


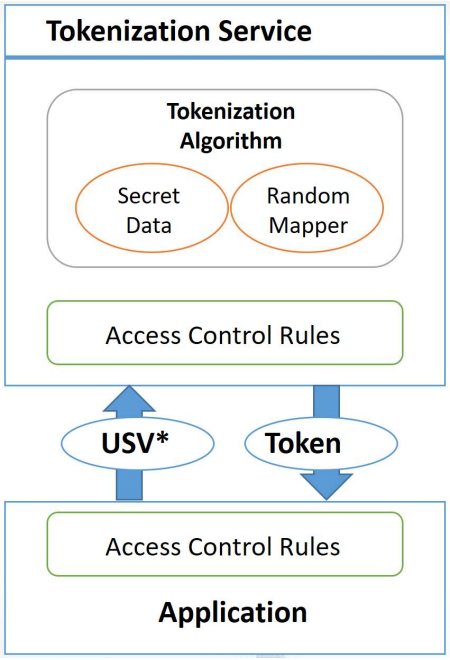
- **Protecting Personally Identifiable Information** (**PII**), including names, addresses, phone, email, policy and account numbers
- **Compliance** with EU Cross Border Data Protection Laws
- Utilizing Data **Tokenization**, and centralized policy, key management, auditing, and reporting

Source: International Customer Case Study

ANSI X9 - CURRENT TOKENIZATION STANDARD

TOKENEX





*: Underlying sensitive value (**USV**)

Accredited Standards Committee X9 Inc.
Financial Industry Standards

Source: ANSI X9

2018 ANSI X9 STANDARD FOR FORMAT PRESERVING ENCRYPTION

TOKENEX

- **Format-preserving encryption (FPE) is useful in situations where fixed-format data, such as Primary account numbers Social Security numbers, must be protected.**

- **FPE will limit changes** to existing communication protocols, database schemata or application code.

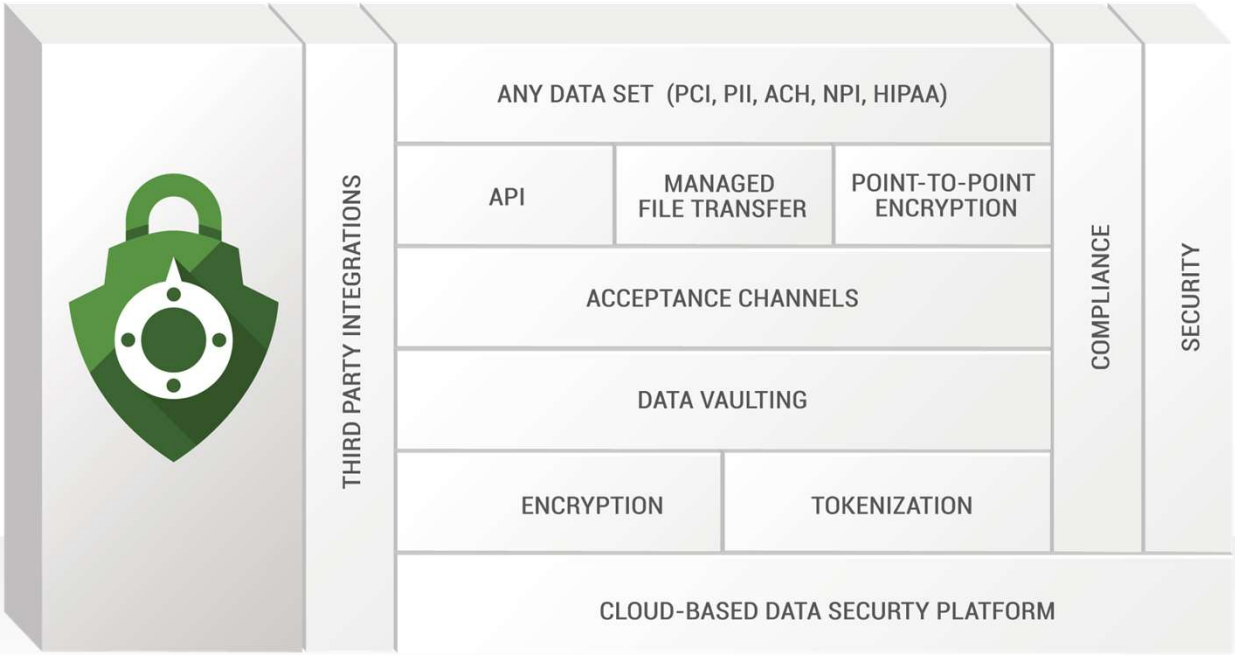
Accredited Standards Committee X9 Inc.
Financial Industry Standards

Source: Accredited Standards Committee ANSI X9

REQUIREMENTS SUPPORTED

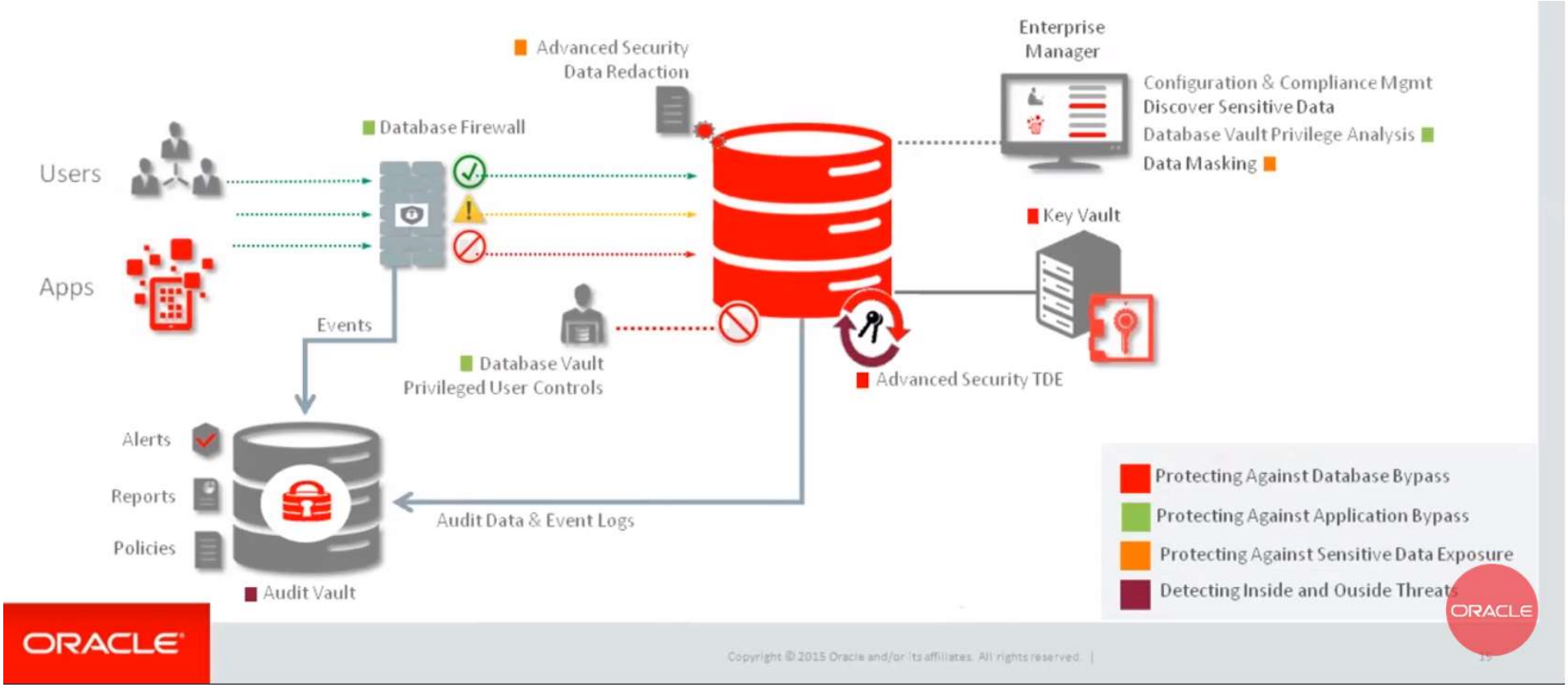
TOKENEX

- Tokenization
- Encryption
- Pseudonymization
- De-identification



Oracle Security Architecture For Data Protection

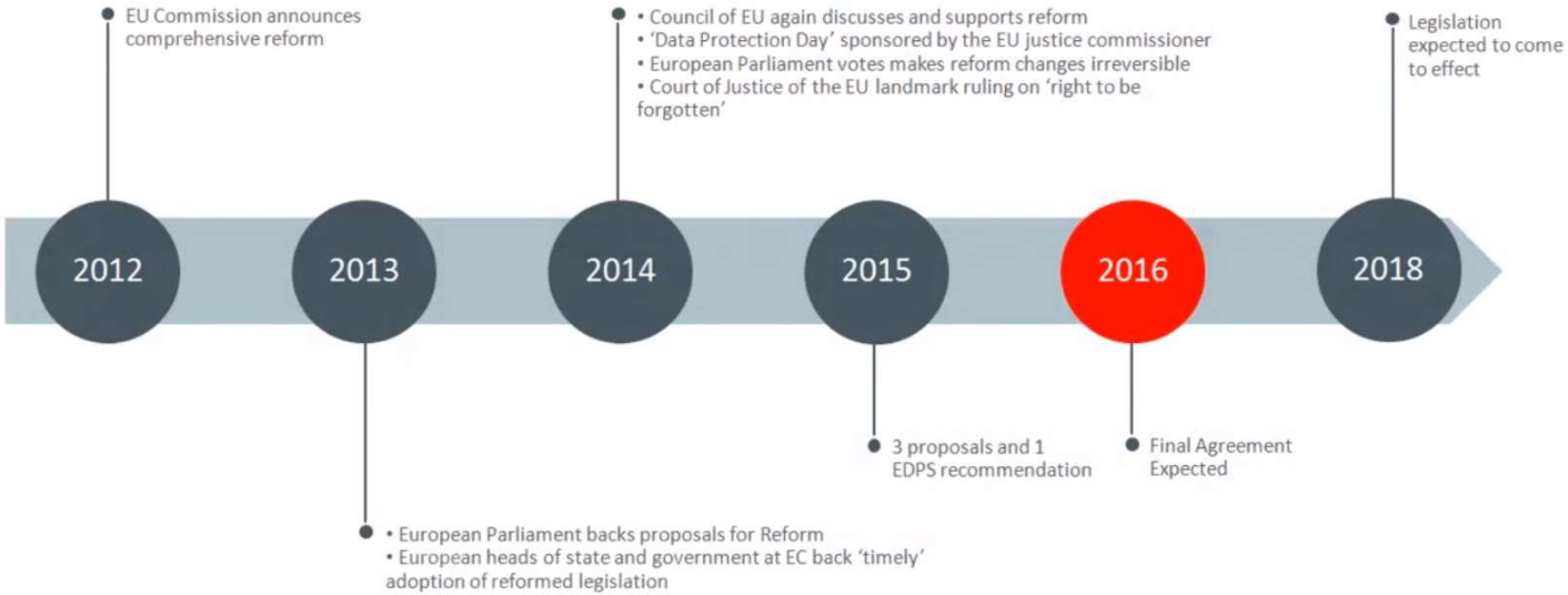
TOKENEX



Source: Oracle

Relevant Timeline

TOKENEX



Source: Oracle