ORACLE

Database Security

Overview

Håkan Råström

Account Client Engineer

Oracle Sweden

Mar 5, 2025

Bruno Reis da Silva

**Technology Account Engineer**

Oracle Sweden

Mar 5, 2025

Safe harbor statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.

Agenda
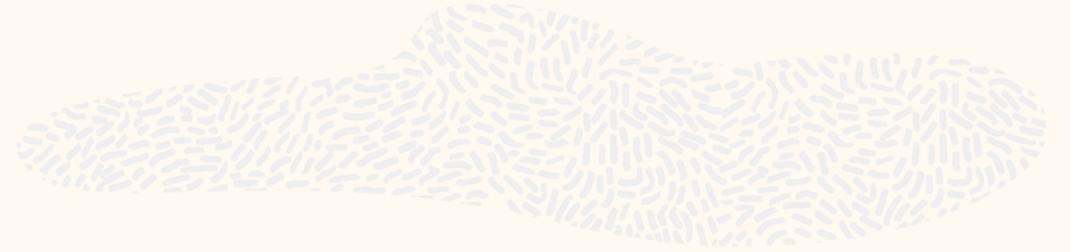
- Why Database security is important

- Asymmetric warfare

- Governance

- Data protection

- Oracle Maximum Availability Architecture (MAA)

- Maximum Security Architecture(MSA)

Why Database security is important

Regulatory Landscape

NCUA
PIPEDA FOIPPA NIS2/DORA RUSSIA RU DPA
FS-ISAC GLBA DPA (UK GDPR) GDPR
HIPAA CIP TSA
CCPA FFIEC CN GDPL
50 STATE DATA PRIVACY LAWS NY DFS500 JP APPI
Patriot Act
Dodd Frank
BASEL III MX LFPDPPP MA DPA BH PDPL IN DPDA HK PDPO
PCI TH PDA
CO DPL NG NDPR SI PDPA
NIST National Institute of Standards and Technology ISO BR LGPD
FedRAMP FIPS 140-2 CI PPL SA POPI AU APP NZ PA
AR PDPL

Compliance & Regulations

Most regulations are technically very similar

- ✓ Maintain secure configuration

- ✓ Monitor access to sensitive data

- ✓ Control access to sensitive data

- ✓ Encrypt the data and manage keys

- ✓ Ensure speedy resumption of services

- ✓ Minimize disruption & data loss

Failing to meet compliance results in fines!

Fine of up to €20M. or 4% of a firm's annual revenue from the preceding year

Fine of up to between € 5-15M or 1-2.5% of the worldwide turnover in the preceding financial year

Daily fines for IT Service Providers of up to 1% of the company's average daily turnover worldwide

Fine up to €10M or 2 % of the total global annual turnover

No organization can afford downtime or cybersecurity incidents

$300,000 Average cost of a single hour of downtime

$4.45M Average cost of a data breach

65% Percentage of data breach victims losing trust in their vendor

Sources: WhipcordEdge; CM Alliance; Breachsense

No organization can afford downtime or cybersecurity incidents

300,000 € Average cost of a single hour of downtime

Is this a high cost ?

Now imagine that the biggest retailer in Finland had 1 hour of downtime. What would be the cost?

>945,000 €

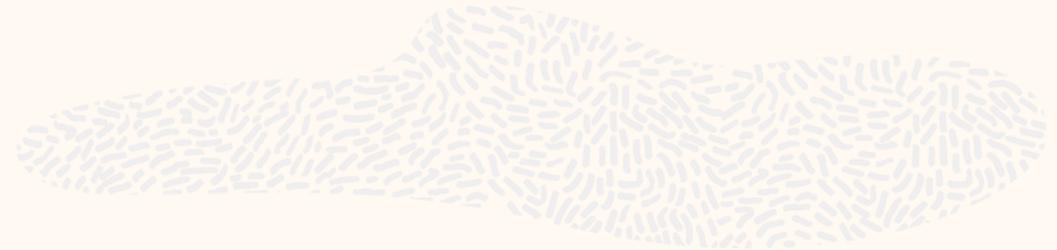Considering only the salary and not other expenses

2 545, 000 € with hourly sales included

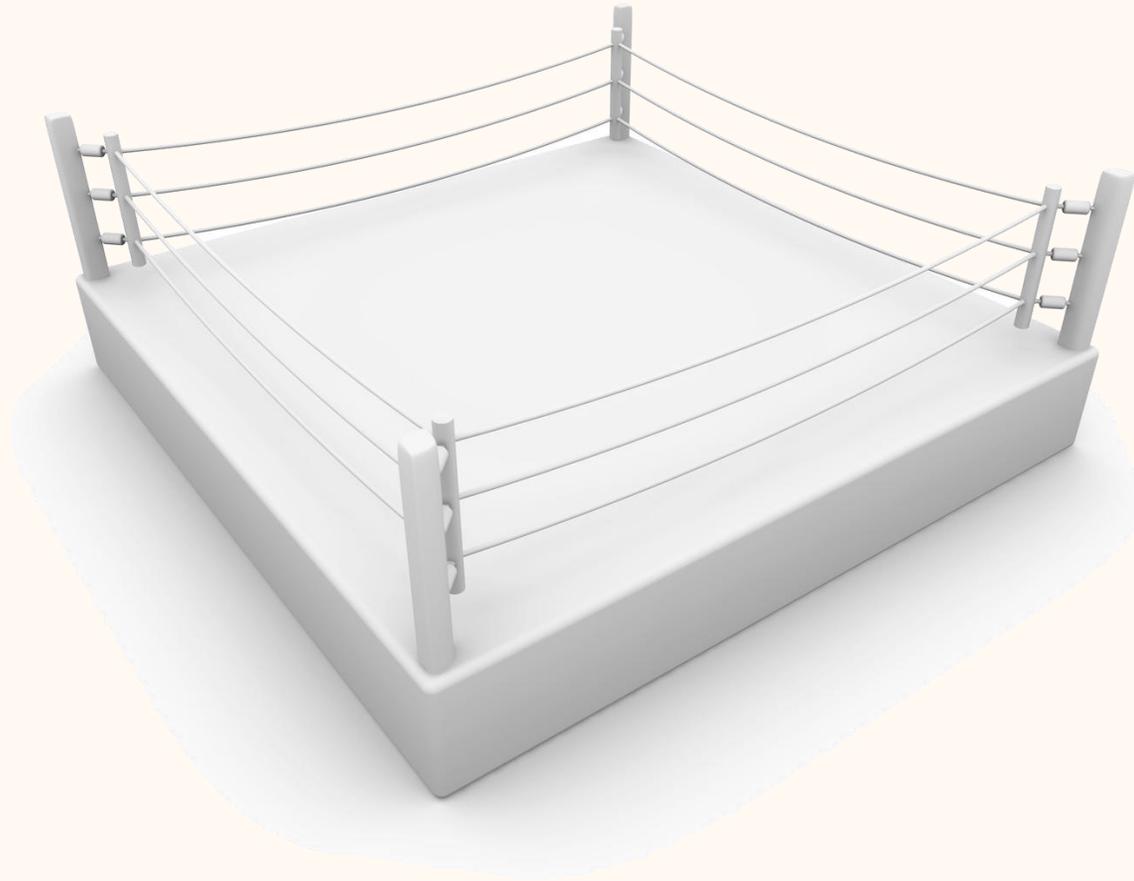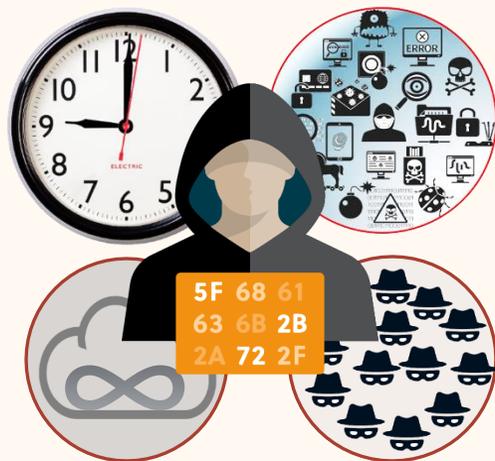# Are there any other reasons WHY we should care about cybersecurity?

Asymmetric warfare
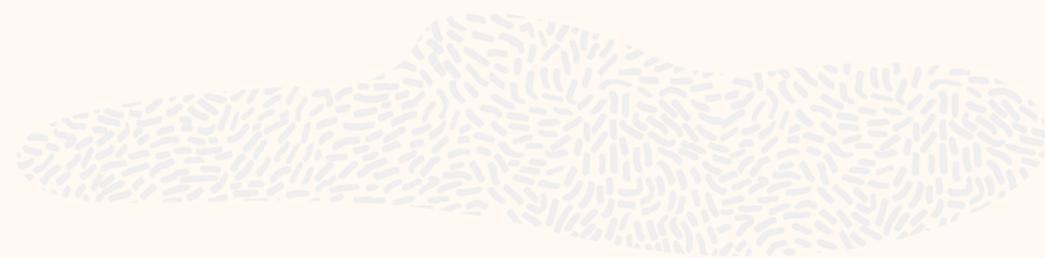
Asymmetric warfare

Challenger's corner

- All the infrastructure
- All the tools
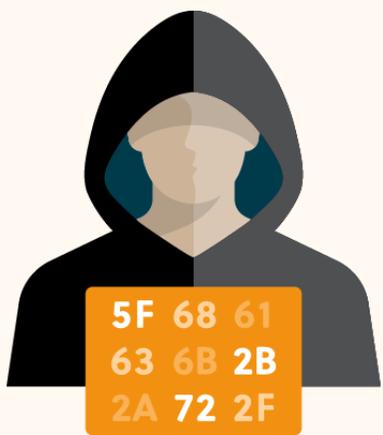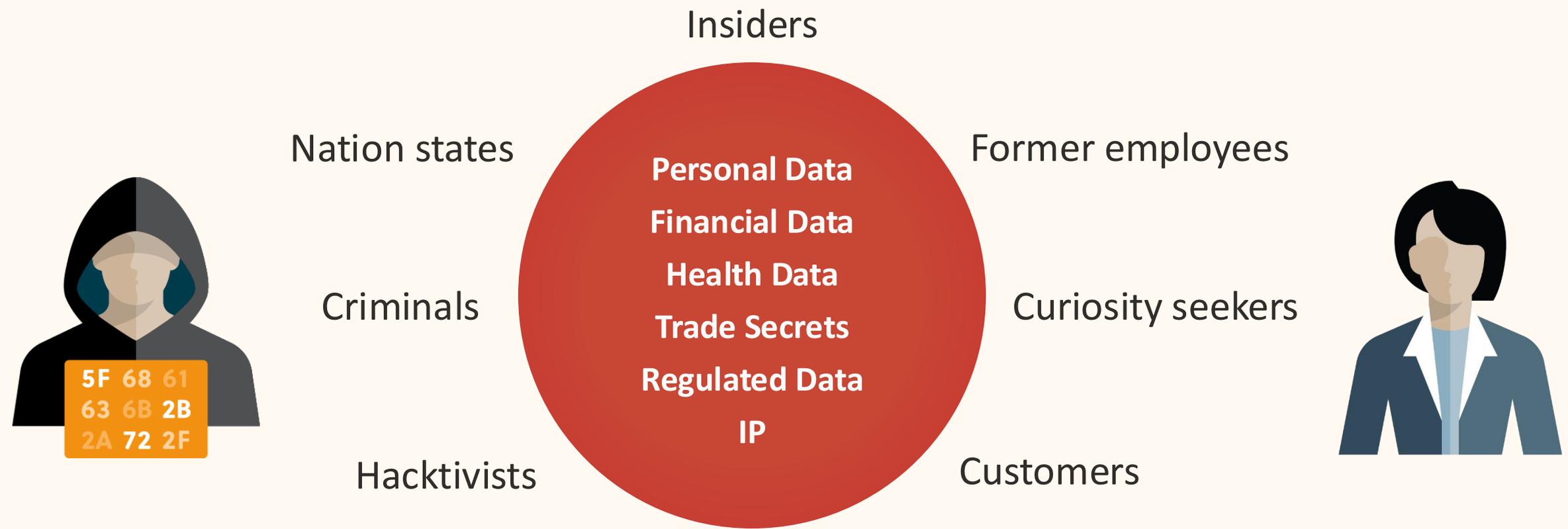- All the time
- A legion of attackers

Defender's corner

- Not enough people
- Not enough resources
- Never enough time

Who wants your data?

Insiders

Nation states

Personal Data
Financial Data
Health Data
Trade Secrets
Regulated Data
IP

Former employees

Criminals

Curiosity seekers

Hacktivists

Customers

Competitors

5F 68 61
63 6B 2B
2A 72 2F

Vastaamo
https://en.wikipedia.org/wiki/Vastaamo_data_breach

AWS
https://firewalltimes.com/amazon-web-services-data-breach-timeline/

Are these our enemies?

Which one can we actually affect?
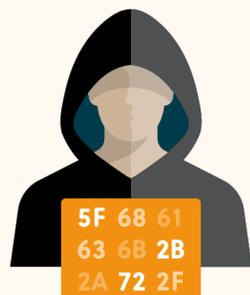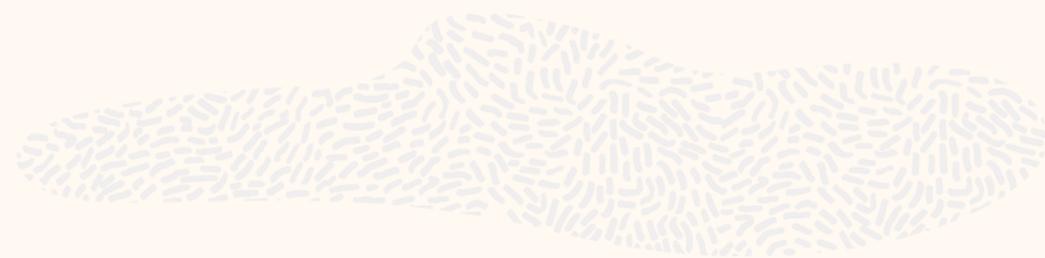
Governance

Governance

Security policies are the backbone of a comprehensive **cybersecurity framework**.
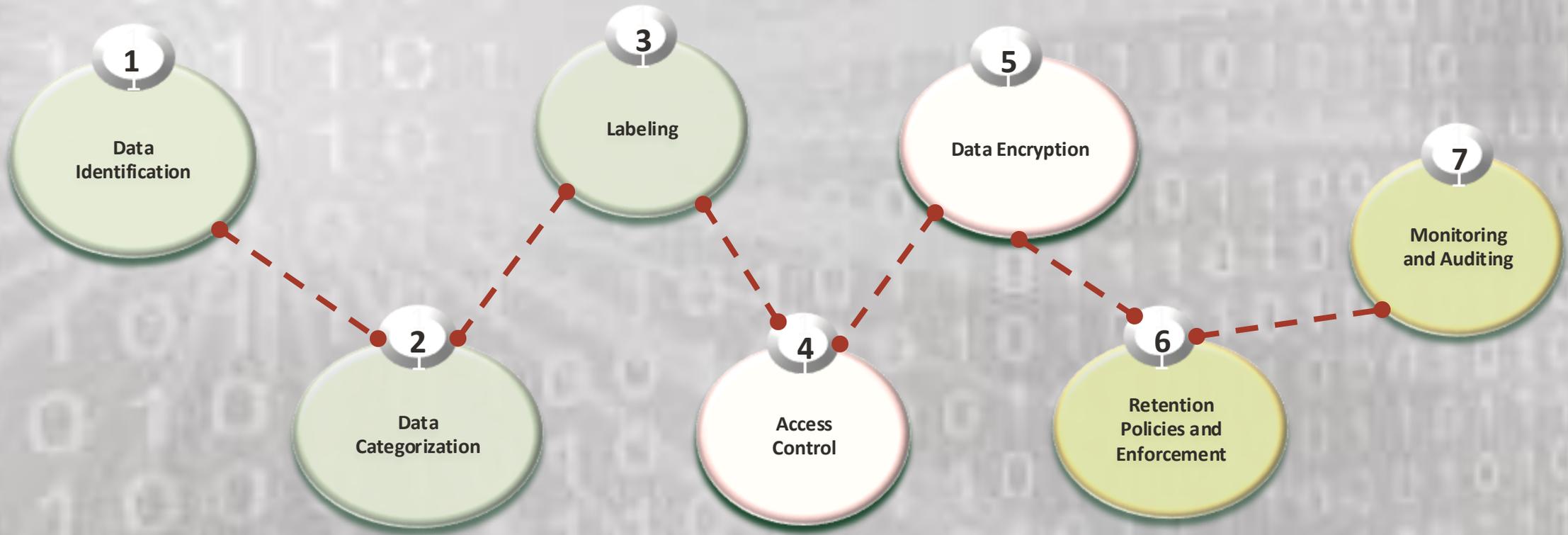
Policies:

- ➤ Establishing Security Standards and Expectations

- ➤ Defining Roles and Responsibilities

- ➤ Supporting Regulatory Compliance

- ➤ Risk Management and Mitigation

Enisa (European Union Agency for Cybersecurity)

https://www.enisa.europa.eu/

Governance

Security policies are the backbone of a comprehensive **cybersecurity framework**.

Data Classification and Handling

1 — Data Identification

2 — Data Categorization

3 — Labeling

4 — Access Control

5 — Data Encryption

6 — Retention Policies and Enforcement

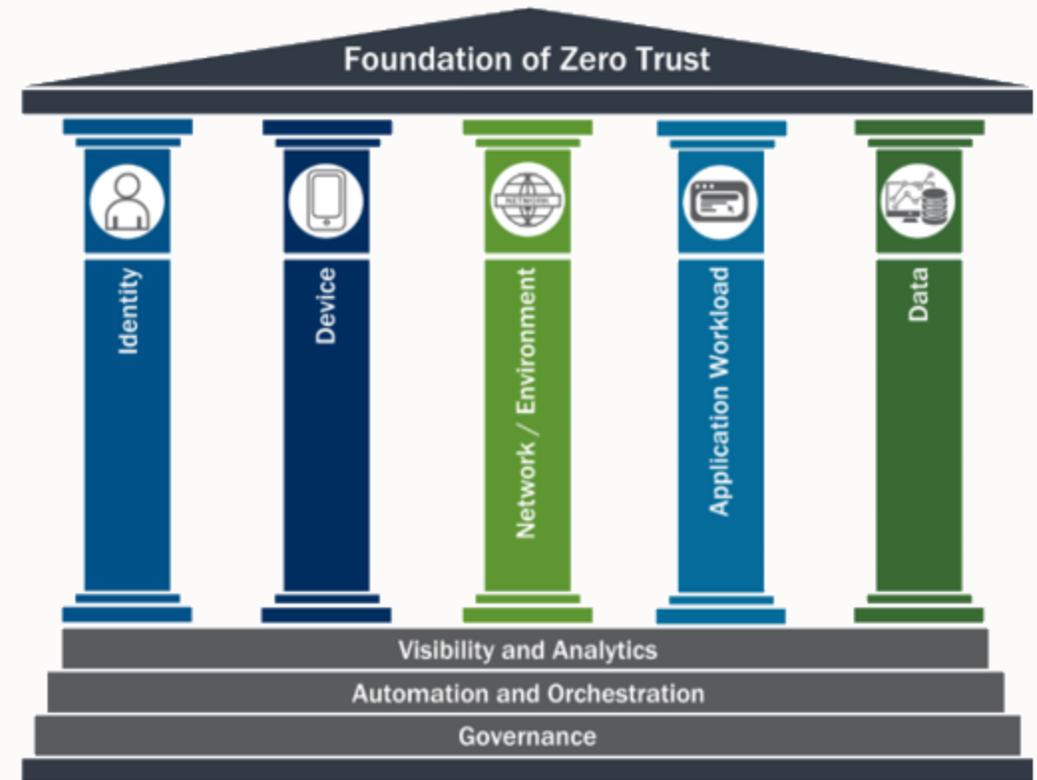**7** — Monitoring and Auditing

Data protection

Block the attack!

Focus on cyber-resilience and the maximum-security architecture

Security "housekeeping" to keep the bad guys out
- Patching & upgrades
- Strengthen authentication
- Least privilege
- Audit activity
- Mask data in test and development systems

Source: CISA Zero Trust Maturity Model (June 2021)

How do you protect the database?

Implement a secure configuration and monitor for configuration drift

- Check configuration against standards/best practices
- Verify that authentication is as strong as practical
- Review user privileges

Encrypt the data and protect the encryption keys

NAMES
ADDRESSES
CREDIT CARDS
HEALTH RECORD
OTHER PII
SECRETS
...
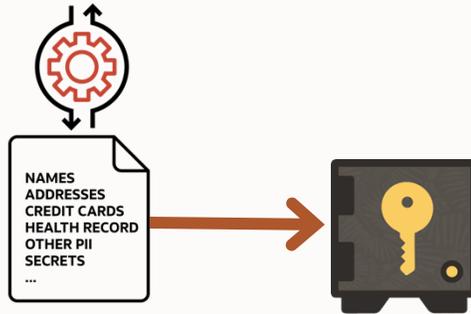
- Encrypt data in motion and at rest
- DO NOT rely on storage level encryption
- Securely manage encryption keys

Control access to the data

- Use database roles and privilege grants
- Control privileged user access
- Enforce separation of duties
- Establish and enforce a trusted path to data
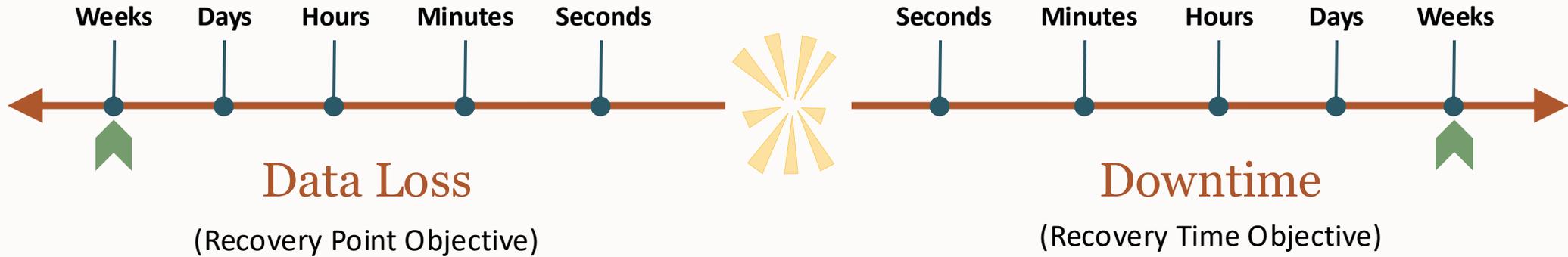
Monitor access to the data

- Use native auditing capabilities to capture high-value activity
- Use network-based monitoring to examine ALL activity

Oracle Maximum Availability Architecture (MAA)

Data Protection Terminology

Recovery Point and Recovery Time Objectives

| Weeks | Days | Hours | Minutes | Seconds | | Seconds | Minutes | Hours | Days | Weeks |

Data Loss
(Recovery Point Objective)

Downtime
(Recovery Time Objective)

Recovery Point Objective (RPO)

Tolerance for data loss (sec's, hours, days); determines frequency of backups and replication approaches

Recovery Time Objective (RTO)

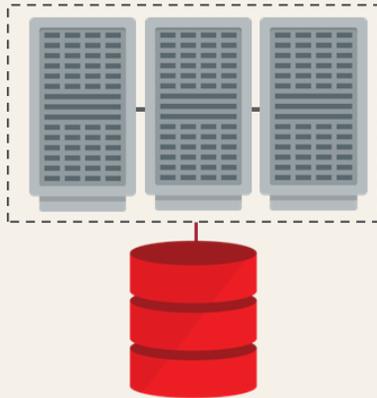The shorter the Recovery Time Objective (RTO) the quicker you get back to business

Data Protection Terminology

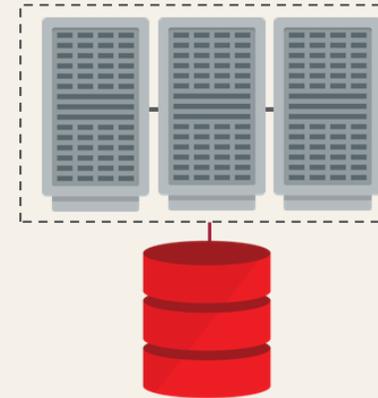High Availability vs. Disaster Recovery for planned *and* unplanned outages

High Availability

- Protect from localized failures (servers, bugs, …)

- Local redundancy

Disaster Recovery

- Protect from site failure (entire data center…)

- Site redundancy

Oracle Maximum Availability Architecture (MAA)

Platinum
Gold
Silver
Bronze

Customer insights and expert recommendations

Reference architectures

24/7
Replication

Production site → Replicated site

HA features, configurations and operational practices

Deployment choices

Generic Systems

Engineered Systems

DBCS ExaCS/ExaCC

Autonomous DB

Continuous availability

Application Continuity

Global Data Services

Data protection

Flashback

RMAN + ZDLRA

Active replication

Active Data Guard

GoldenGate

Scale out

RAC

ASM

Sharding

https://docs.oracle.com/en/database/oracle/oracle-database/23/haiad/maara_overview.html

Oracle Maximum Security Architecture(MSA)

Governance

Security policies are the backbone of a comprehensive **cybersecurity framework**.

Data Classification and Handling

1
Data Identification

2
Data Categorization

3
Labeling

4
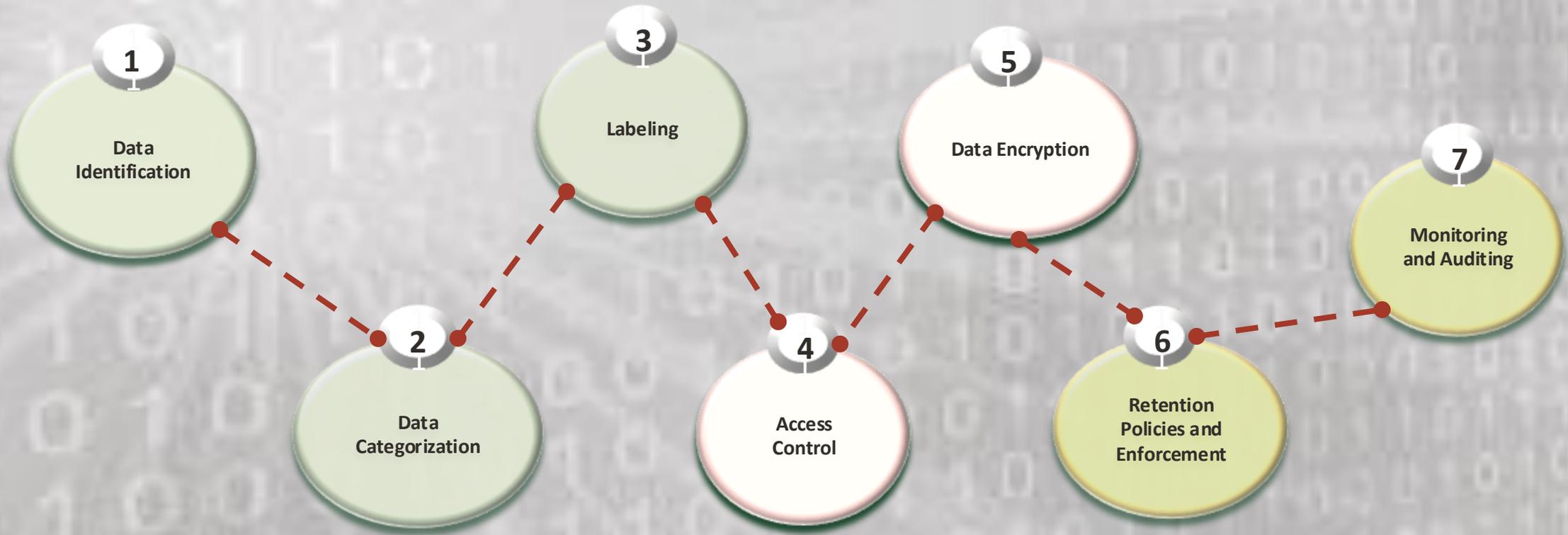**Access Control**

5
Data Encryption

6
Retention Policies and Enforcement

7
Monitoring and Auditing

Comprehensive security controls for Oracle Databases

Assess

Config-Assessment(DBSAT, DBLM, Data Safe)
Data Discovery
Privilege Analysis*

Detect

Activity Auditing
Audit Vault (NIS2, GDPR, HIPAA…)
Database Firewall*

Prevent

Transparent Data Encryption & Key Vault
Data Masking, Data Redaction
Database Vault*
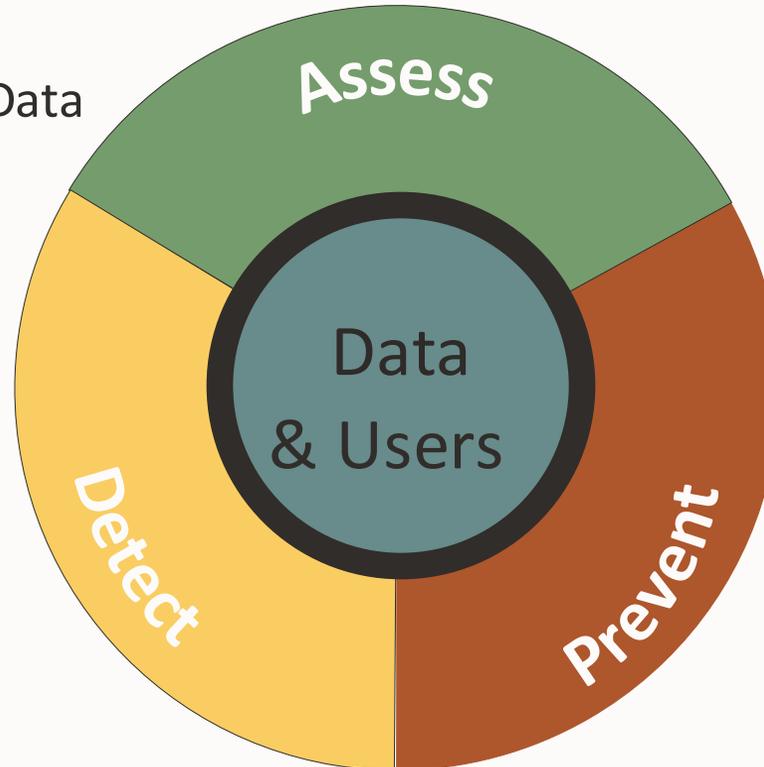
Data

Label Security
Virtual Private Database (VPD)
Real Application Security (RAS)*
DB Cryptographic Toolkit

Users

Password, PKI, Kerberos, Radius
Proxy Users, Password Profiles
Roles and Privileges
Oracle & Active Directory

* Unique to Oracle

Maximum Security Architecture

Key to Database Security Controls
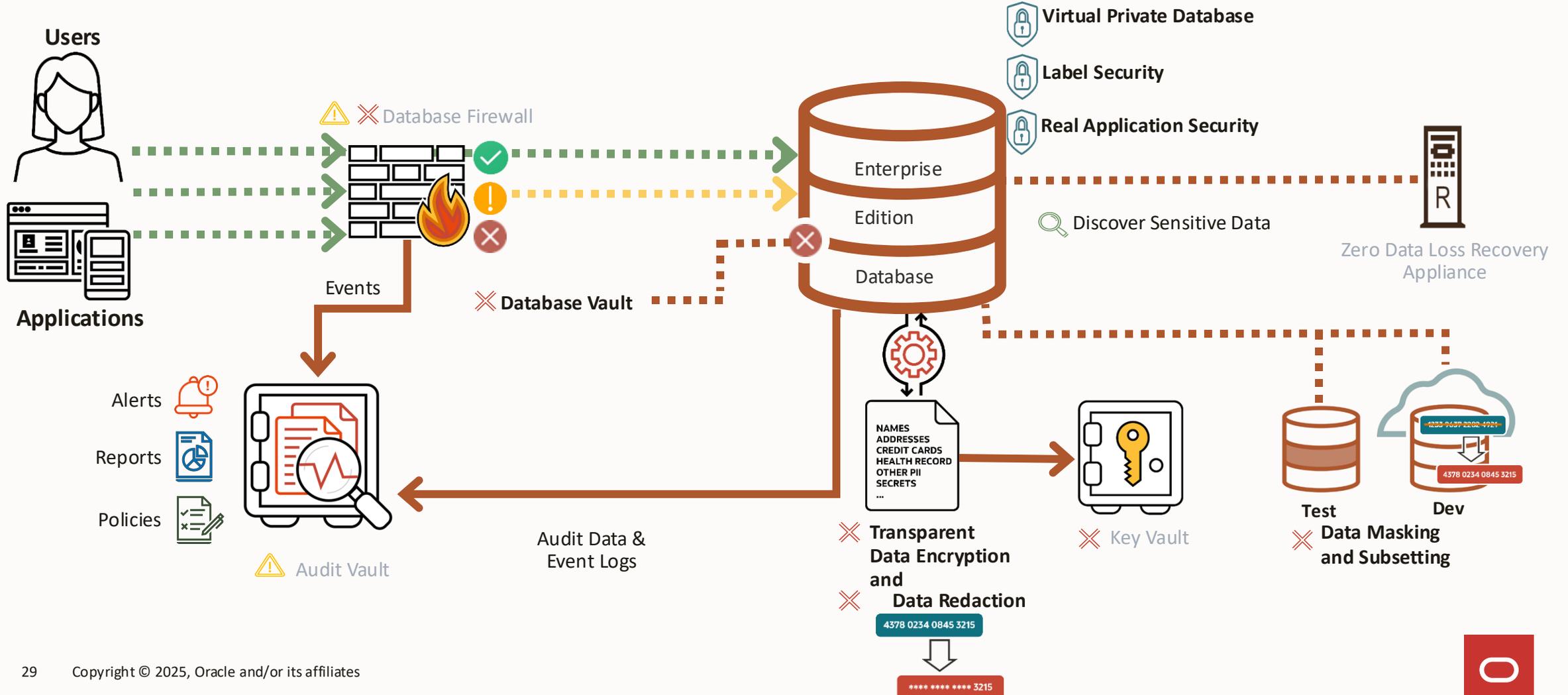
Assess   Prevent   Detect

Data-Driven Security

Users

Applications

Database Firewall

Events

Database Vault

Virtual Private Database

Label Security

Real Application Security

Enterprise
Edition
Database

Discover Sensitive Data

Zero Data Loss Recovery Appliance

Alerts

Reports

Policies

Audit Vault

Audit Data &
Event Logs

NAMES
ADDRESSES
CREDIT CARDS
HEALTH RECORD
OTHER PII
SECRETS
...

Transparent Data Encryption and Data Redaction

4378 0234 0845 3215

**** **** **** 3215

Key Vault

Test

Dev

4378 0234 0845 3215

Data Masking and Subsetting

Maximum Security Architecture

Assess Prevent Detect

Data-Driven Security

Users

Virtual Private Database

Label Security

Real Application Security

Network Encryption
TLS*

Enterprise

Edition

Database

Discover Sensitive Data
Oracle Database Security Assessment Tool

Applications

✕ **Database Vault**

NAMES
ADDRESSES
CREDIT CARDS
HEALTH RECORD
OTHER PII
SECRETS
...

Test

Dev

✕ **Data Masking and Subsetting**

4378 0234 0845 3215

✕ **Transparent Data Encryption and**
✕ **Data Redaction**

4378 0234 0845 3215

**** **** **** 3215

Learn More

Oracle.com: www.oracle.com/security/database-security/

Blog: http://blogs.oracle.com/cloudsecurity/db-sec

NEW: eBook 6th Edition: www.oracle.com/securingthedatabase

Oracle LiveLabs - Try it yourself:

- Database Security: https://bit.ly/golivelabsdbsec

AskTOM Office Hours offers free, open Q&A sessions with Oracle Database PM/experts. We hold a LIVE session on the second Wednesday of each month, at 15:00 UTC

https://bit.ly/asktomdbsec
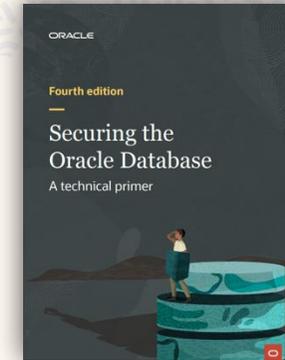
Oracle LiveLabs

NIS2 EU Directive Product Mapping – Database Security

Articles / Recitals	Topics	Products / Features
Recital 49, 50	On **cyber hygiene** policies	• DBSAT, Data Safe, AVDF, User Profiles
Recital 51, 104	Broadly on **detection and prevention** of cyberattacks	• All
Recital 54	Policy to address **Ransomware**	• Advanced Security (TDE), OKV, ZDLRA & more
Recital 79	Broadly on threats to security	• Database Vault – prevent human error
Recital 57, 58, 77, 78 Article 20	Broadly on **Assessments**	• DBSAT, Data Safe, AVDF, training on Assessing a database
Recital 89	Broadly on **Zero Trust**	• All
Recital 98	End-to-end **Encryption**	• Advanced Security, NNE, TLS
Article 21	Broadly on **prevent or minimise the impact of incidents**	• DBSAT, ZDLRA, ASO, OKV, MFA, TLS/NNE
Article 23	Broadly on **reporting obligations / notification on incidents**	• AVDF, Data Safe
Article 32, 33	Broadly on **competent authorities powers**	• DBSAT, AVDF, Data Safe - prepare for audits

NIS2 EU Directive Product Mapping – Cloud Systems

Articles / Recitals	Topics	Products / Features
Recital 51	Broadly on **prevention of cyberattacks**	• ZFS Storage Appliance (ZFS), Zero Data Loss recovery Appliance (ZDLRA)
Recital 54	Broadly on **Ransomware**	• ZFS, ZDLRA
Recital 57, 58, 77, 78	Broadly on **assessments of active cyber protection**	• ExaCHK, Healthcheck, Data Protection Assessment, Recovery Health Dashboard
Recital 89	Broadly on **Zero Trust**	• Exadata Database Machine (Exadata), ZDLRA, Exadata Cloud@Customer,
Recital 98	Broadly on **end-to-end encryption**	• Exadata Cloud@Customer, ZDLRA*
Article 21 ([2c, 2h])	Broadly on **business continuity** and **encryption**	• ZFS, ZDLRA, Exadata Cloud@Customer, Exadata
Article 21 ([2i])	Broadly on **Access Management**	• ZFS, ZDLRA, Exadata Cloud@Customer,

NIS2 EU Directive Product Mapping - IAM

Articles / Recitals	Topics	Products / Features
Recital 54,56	Emphasis on need for Member States policy addressing the rise of ransomware attacks as part of their national cybersecurity strategy, ensuring also protection of small and medium businesses.	• OIG, OAM, ODS • OCI IAM • OAG
Recital 89	Emphasis on zero trust, identity and access management and using of machine learning and artificial intelligence as cybersecurity enhancing technologies	• OIG, OAM, ODS • OCI IAM • OAG
Article 19, 29, 30	Broadly on **assessments (supervision)**	• OIG • OAG
Article 21	Emphasis on **human resources security, access control policies and asset management;** Emphasis on the use of **multi-factor authentication or continuous authentication solutions**	• OIG, OAM, ODS • OCI IAM • OAG
Article 25	**Encourage the use of European and international standards and technical** specifications relevant to the security of network and information systems	• OIG, OAM, ODS • OCI IAM • OAG

Our mission is to help people see data in new ways, discover insights, unlock endless possibilities.