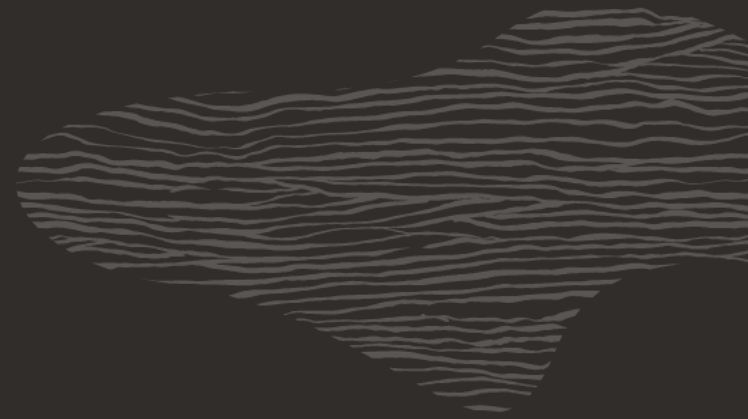
ORACLE



Архитектура максимальной безопасности баз данных Oracle

Securing data at its source

Николай Данюков

Ведущий консультант, Oracle СНГ

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.

Регулирование и утечки

Россия

Роскомнадзор ФСБ ФСТЭК

Технологии и медиа, 15 октября 2020, 17:00

Более 90% компаний из России столкнулись с утечками данных

В большинстве случаев причиной разглашения конфиденциальных данных становятся сотрудники, которые намеренно передают их на сторону. Чаще всего утекают техническая информация и бухгалтерские документы

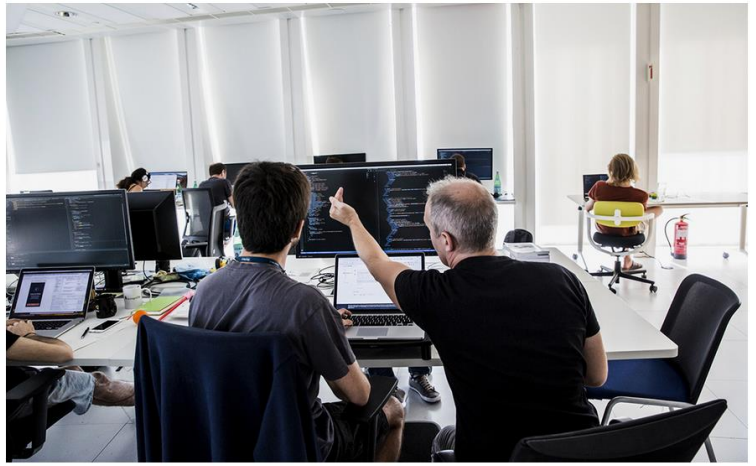


Фото: Angel Garcia / Bloomberg

«… в **60%** случаев причиной стали намеренные действия сотрудников, остальные **40%** таких ситуаций произошли по причинам их невнимательности и наивности…»

Регулирование и утечки

У семи нянек …

- Следует забыть принцип 80:20
- 99% усилий организаций сосредоточено на прохождении аудита
- 99% денег, потраченных на безопасность, сосредоточено на:
  - Соблюдение государственных и отраслевых нормативов
  - Аудит, который не является безопасностью и по существу не имеет отношения к безопасности

General Data Protection Regulation

Office of the Privacy Commissioner of Canada

PCI

и др.

- Краткий перечень организаций, взломанных в последнее время

Каждая организация … Все … прошли свои проверки

Информационная безопасность

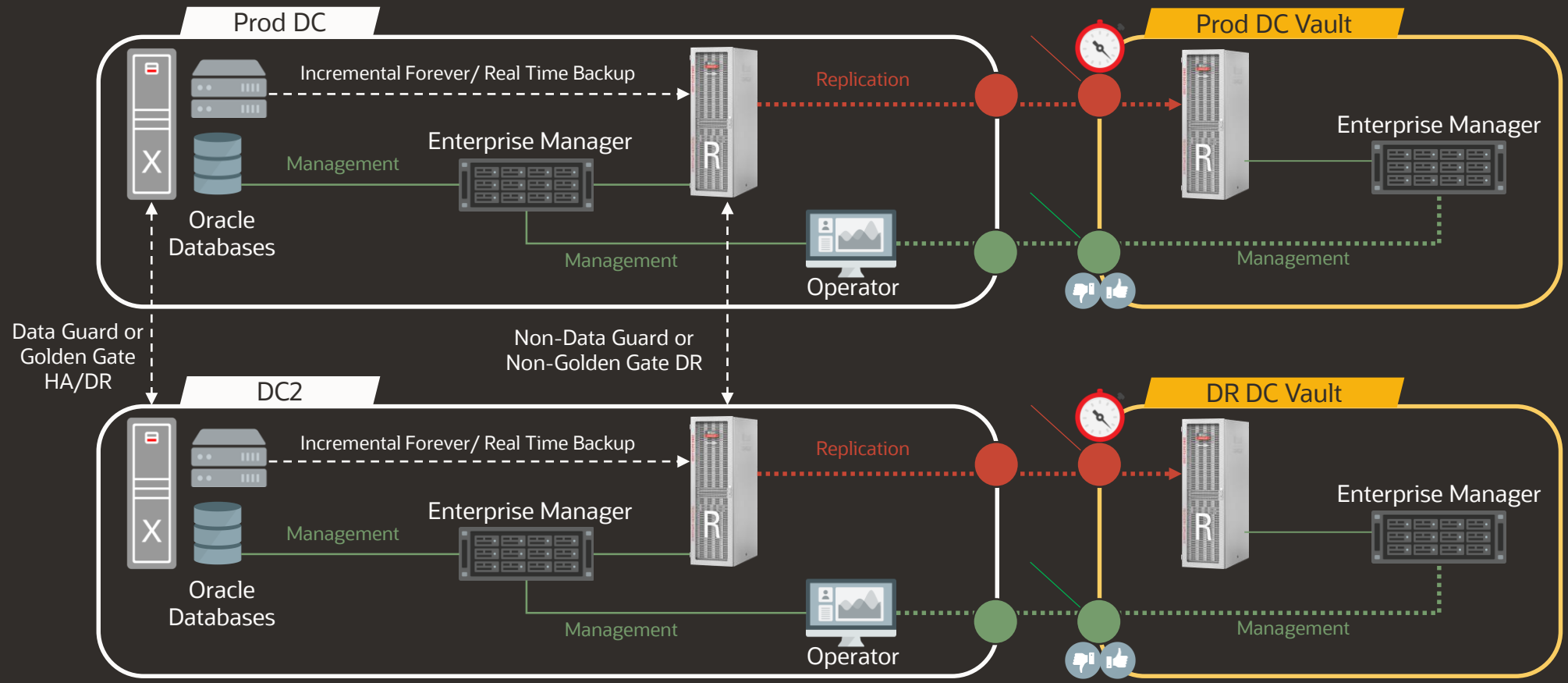
Целостность,

Обеспечение достоверности и полноты информации и методов ее обработки

Доступность,

Обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости

Recovery Appliance Cyber Security Architecture

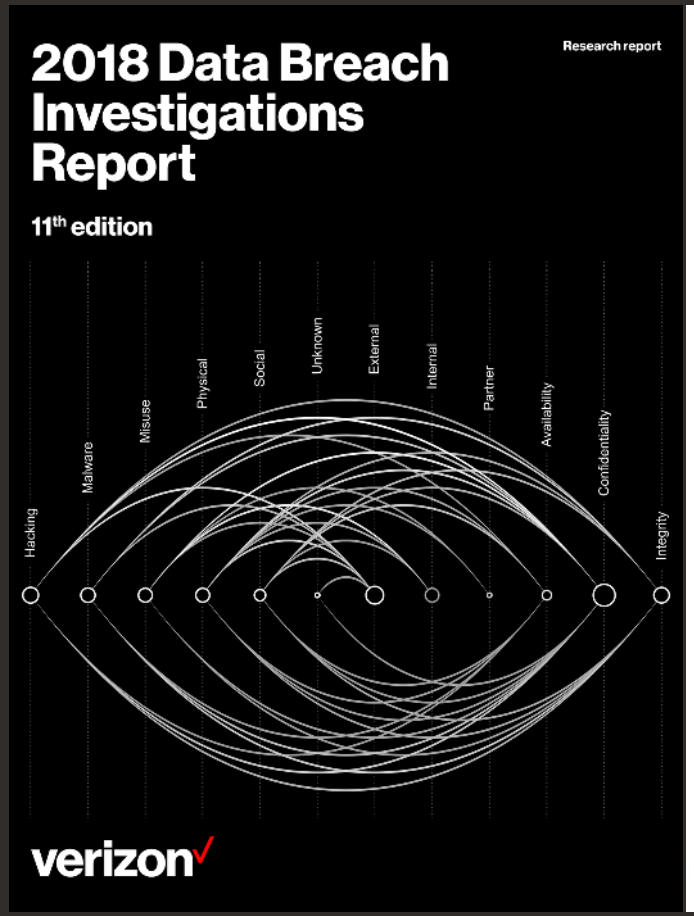


Webinar

Информационная безопасность

Конфиденциальность,
Обеспечение доступа к информации только авторизованным пользователям

База данных - предпочтительная цель для атак



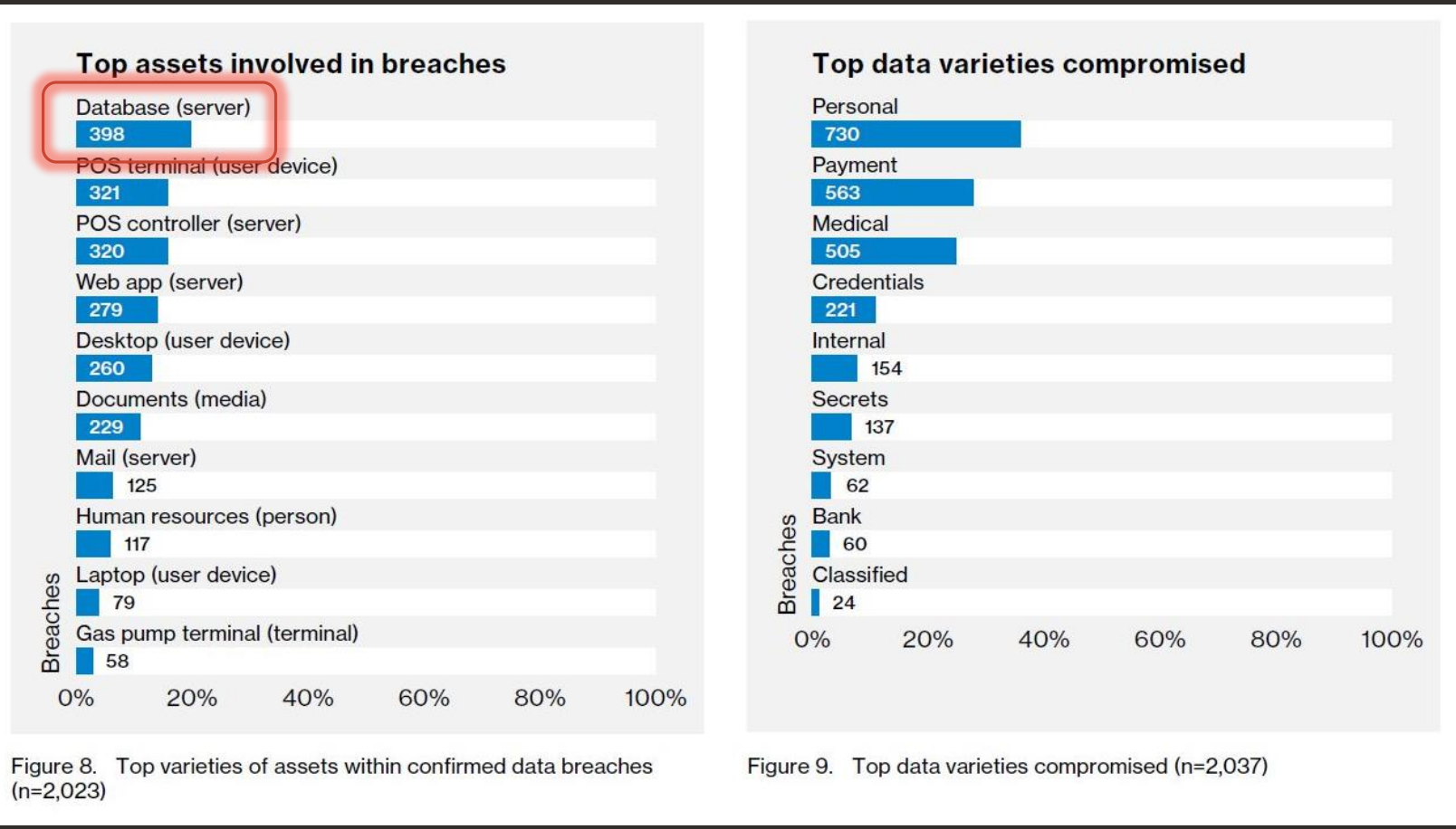


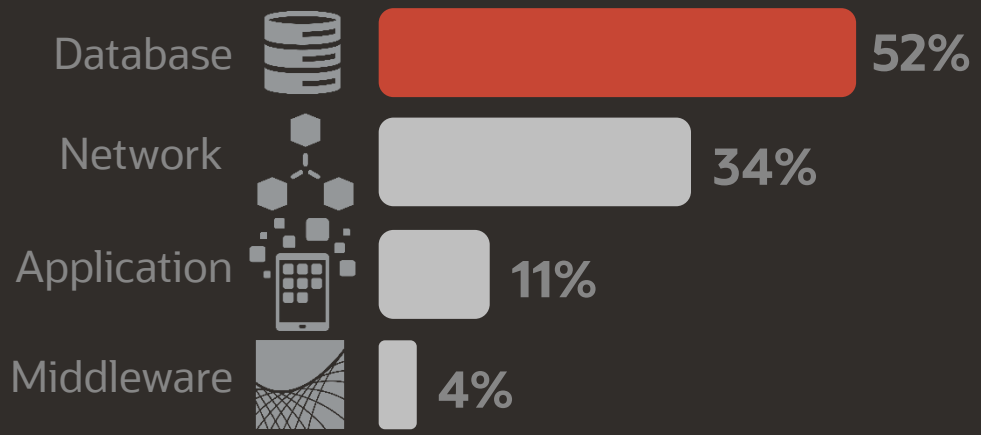
Figure 8. Top varieties of assets within confirmed data breaches (n=2,023)

Figure 9. Top data varieties compromised (n=2,037)

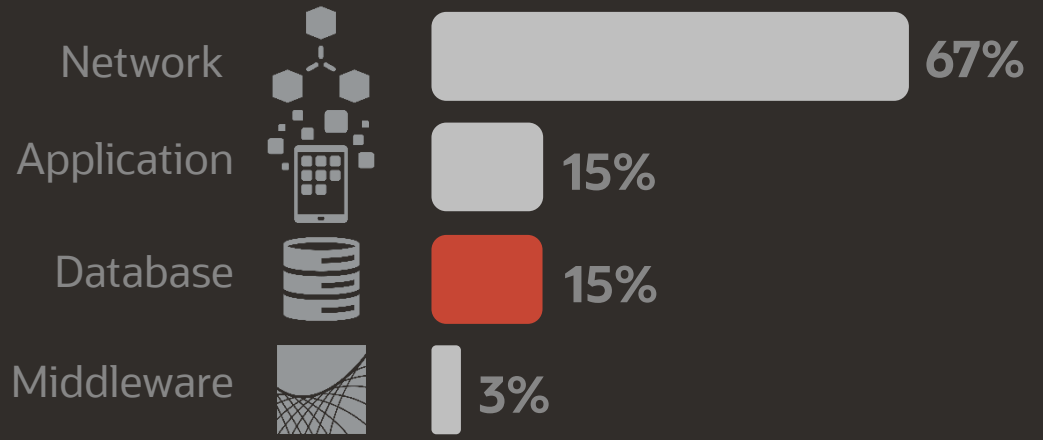
База данных - предпочтительная цель для атак

Защита с использованием "периметра ИБ"

Оценка уязвимости элементов IT



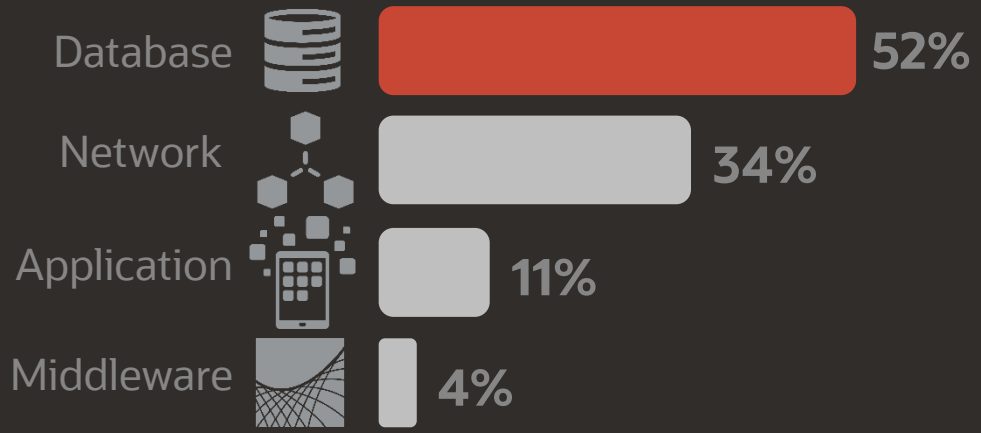
Затраты на противодействие утечкам



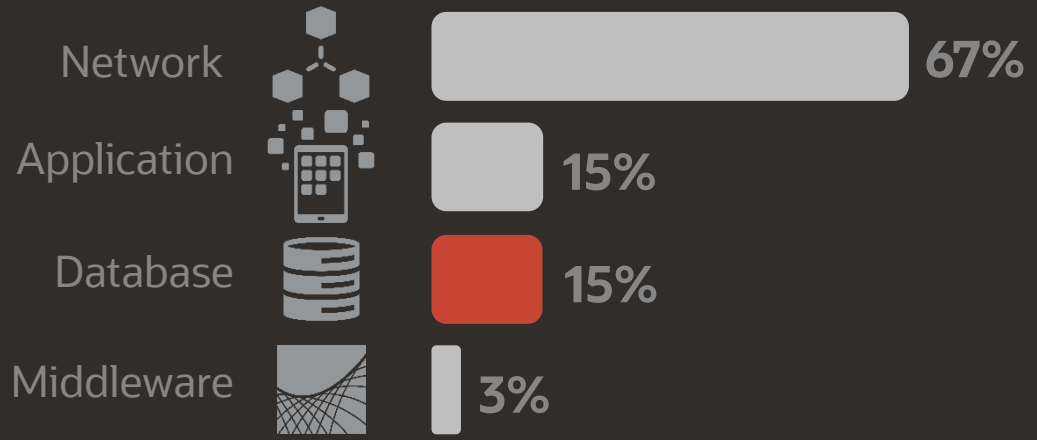
База данных - предпочтительная цель для атак

Требуется защита не только периметра, но и внутренней инфраструктуры

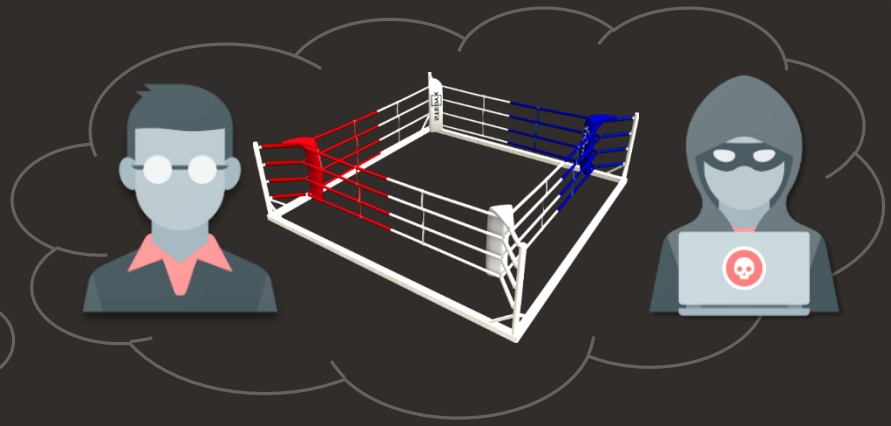
Оценка уязвимости элементов IT



Затраты на противодействие утечкам



Аргументы, чтобы ничего не делать



- Наш сетевой брандмауэр - достаточная защита
- Нарушения вряд ли произойдут у нас
- Мы открытая компания, наши данные никому не интересны
- Мы полностью доверяем нашим сотрудникам
- Мы прошли внутренний аудит

Исход «поединка» за владение информацией вполне предсказуем

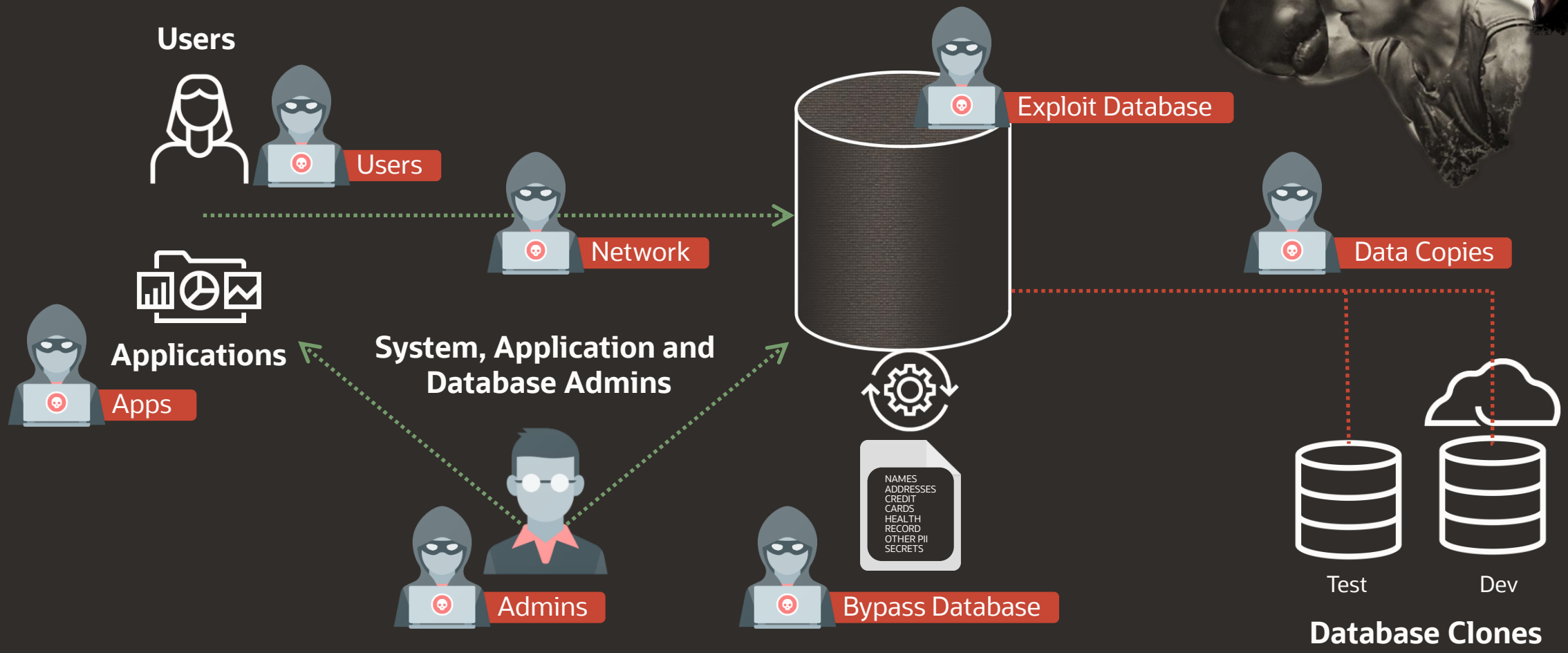
Претендент (злоумышленник)

- Вся инфраструктура
- Все время
- Все инструменты
- Легион нападающих

Защитник (невнимательный и наивный)

- Никогда не хватает времени
- Не хватает людей
- Недостаточно ресурсов

Как хакеры атакуют базы данных?



Baseline Security (Обеспечение базового уровня безопасности) (1)

Элементы управления безопасностью базы данных

Оценка соответствия Превентивная защита Обнаружение

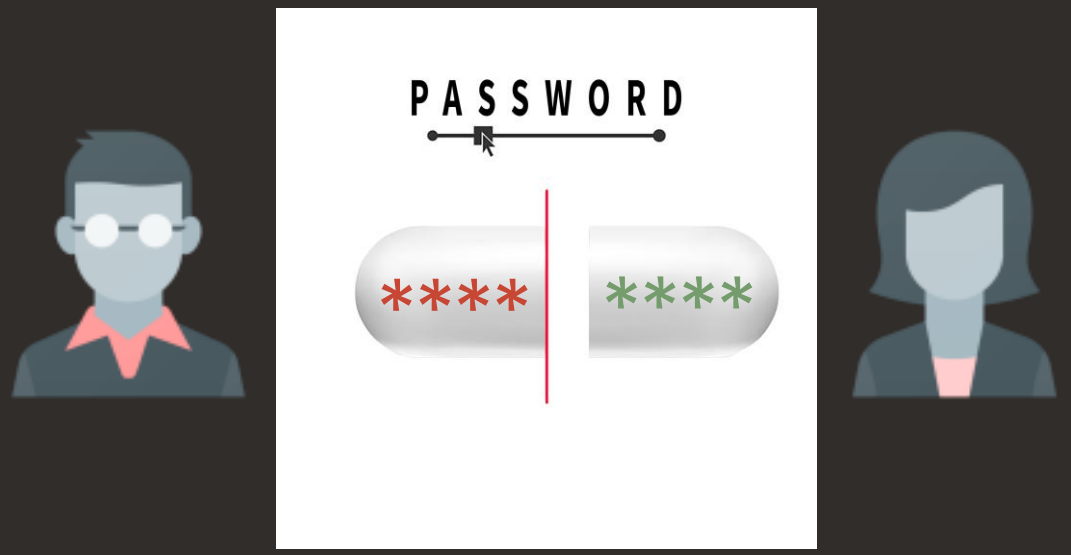
Миллиарды «утечек» из-за плохой парольной защиты

Наихудшие пароли в 2018 году

«Креативная» аутентификация по паролю

Проблема: Хранение паролей

From a headache From a diarrhoea



Security “Life Hack”

Даже хорошие пароли могут быть украдены…

Почти каждый DBA пишет и использует различные скрипты для автоматизации процедур мониторинга и резервного копирования баз данных Oracle.

```
#!/bin/bash
RETVAL=`sqlplus -silent scott/tiger <<EOF
SET PAGESIZE 0 FEEDBACK OFF VERIFY OFF
HEADING OFF ECHO OFF
SELECT * FROM emp;
EXIT;
EOF`
if [ -z "$RETVAL" ]; then
  echo "No rows returned from database"
  exit 0
else
  echo $RETVAL
fi
```

Даже хорошие пароли могут быть украдены…

Почти каждый DBA пишет и использует различные скрипты для автоматизации процедур мониторинга и резервного копирования баз данных Oracle.

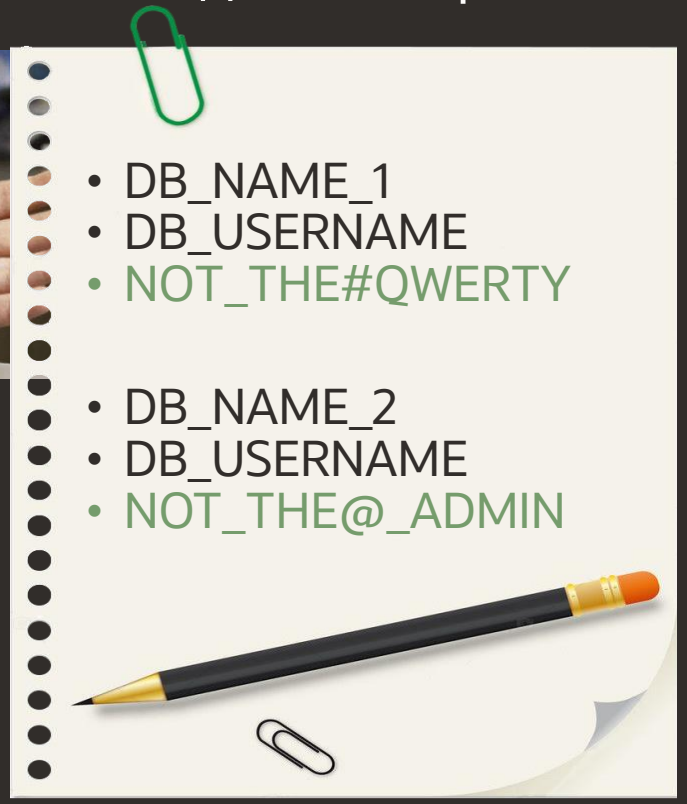
```
#!/bin/bash
export DB_USER=backup_user
export DB_PASS='~/.secure_pwd_extractor'
$ORACLE_HOME/bin/rman << EOF
  connect target $DB_USER/$DB_PASSWORD
  shutdown immediate;
  startup mount;
  backup spfile;
  backup database;
```

SEPS - “Oracle Secure External Password Store”
Технология, доступна начиная с Oracle 10gR2

Технология “Oracle Secure External Password Store” (SEPS) (1)

Сравнение с другими способами хранения паролей

CUSTOM: Данные “надежно” спрятаны



~/.secure_pwd_extractor

Технология “Oracle Secure External Password Store” (SEPS) (2)

Сравнение с другими способами хранения паролей

CUSTOM: Данные “надежно” спрятаны

- DB_NAME_1
- DB_USERNAME
- NOT_THE#QWERTY

- DB_NAME_2
- DB_USERNAME
- NOT_THE@_ADMIN

~/.secure_pwd_extractor

SEPS: Данные зашифрованы 3DES

List credential (index: connect_string username)

#	Connect_string	Username	PWD
1	ORCL	scott	XXXXX
2	localhost:1521/ORCL	monitoring_user	XXXXX
3	127.0.0.1:1521/ORCL	batch_reporting	XXXXX

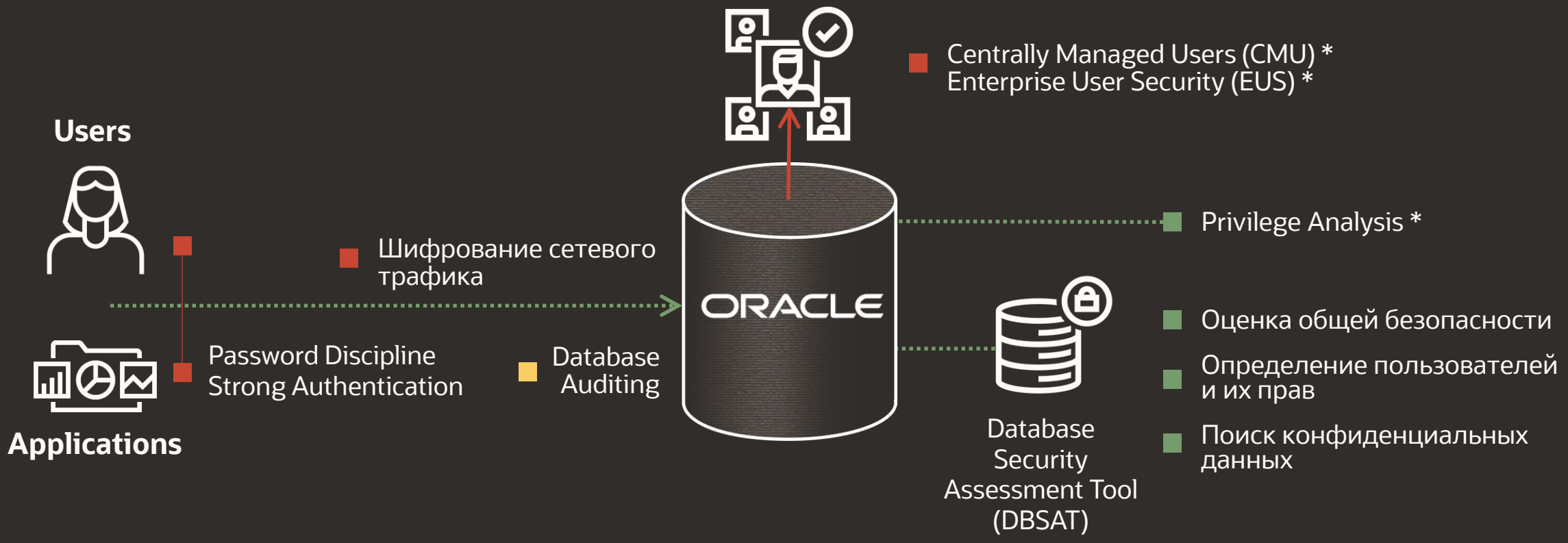
Password

- ewallet.p12
- cwallet.sso

Пример подключения к СУБД ORACLE от имени пользователя ‘SCOTT’

```
$ sqlplus /@ORCL
```

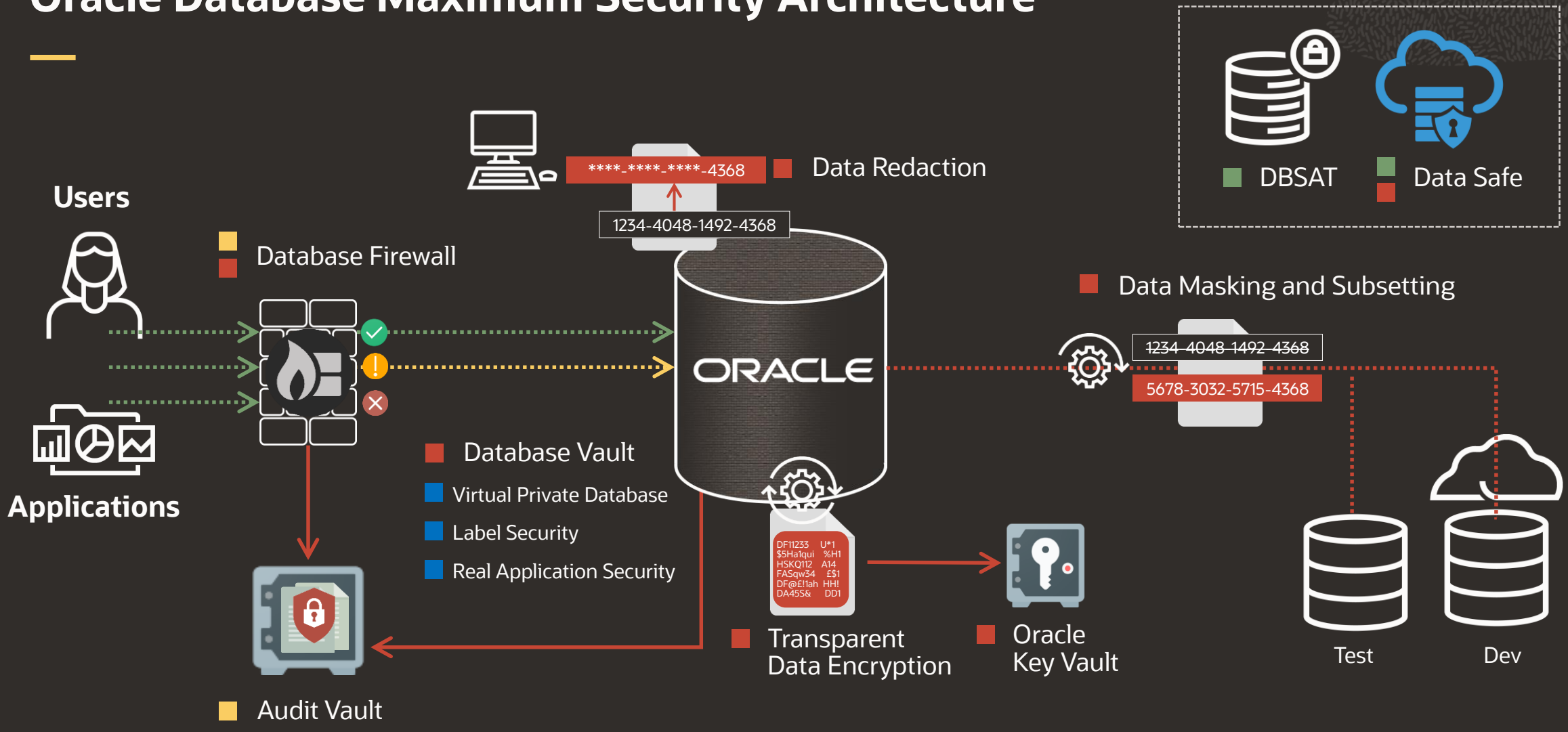
Baseline Security (Обеспечение базового уровня безопасности) (2)



* *Доступно только в версии Enterprise Edition*

Оценка соответствия Превентивная защита Обнаружение

Oracle Database Maximum Security Architecture



DBSAT & Data Safe

AVDF

ASO

Key Vault

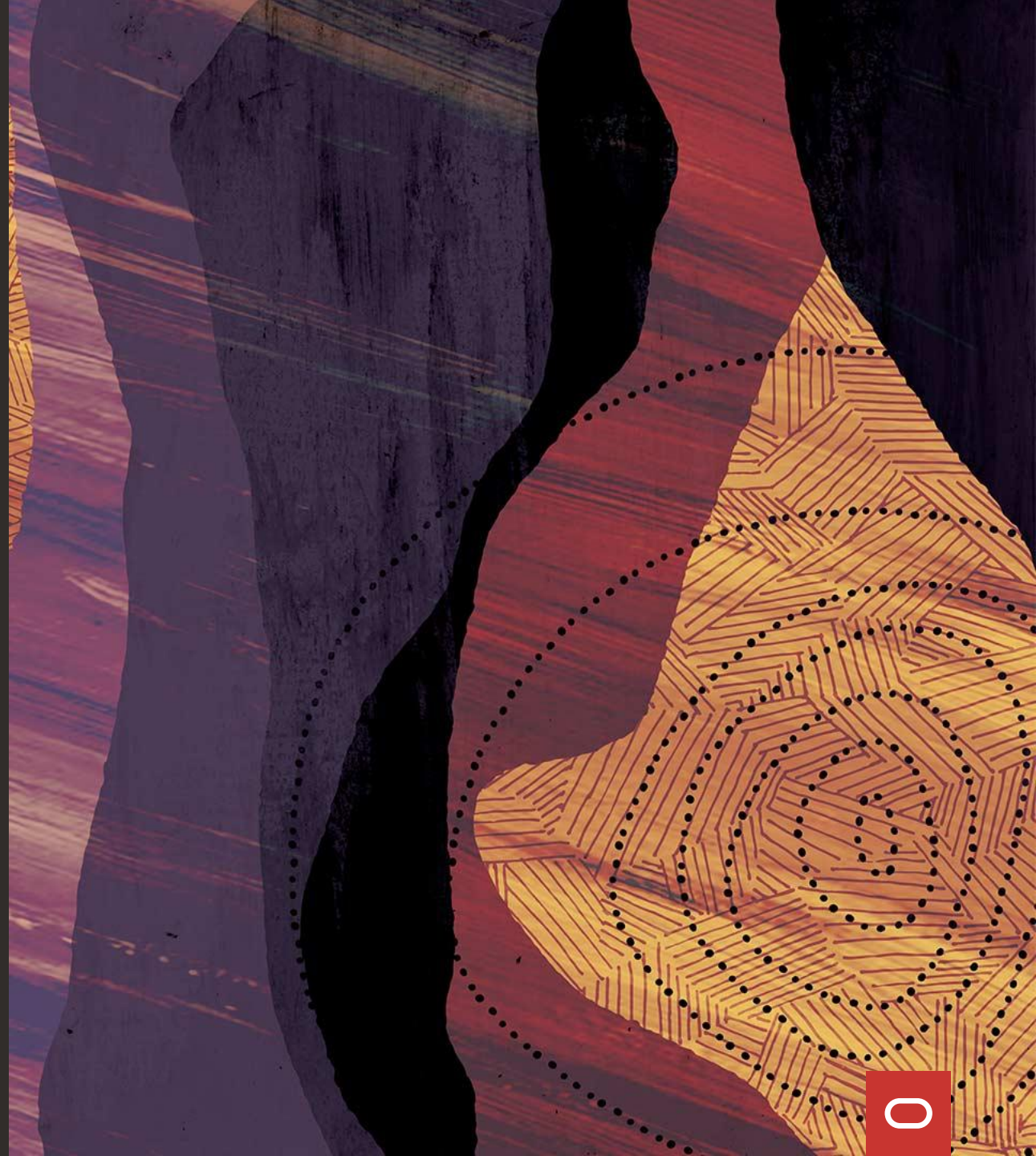
Masking Pack

Label Security

DBV

Спасибо

Николай Данюков
Ведущий консультант, Oracle СНГ



ORACLE