MOSCOW ft meet up online

ЦФТ ЦЕНТР ФИНАНСОВЫХ ТЕХНОЛОГИЙ

ORACLE

Обеспечение безопасности БД Oracle

Без изменений производительности и бизнес-приложений

Николай Данюков

Ведущий консультант, Oracle в России и СНГ

25 ноября, 2020

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.

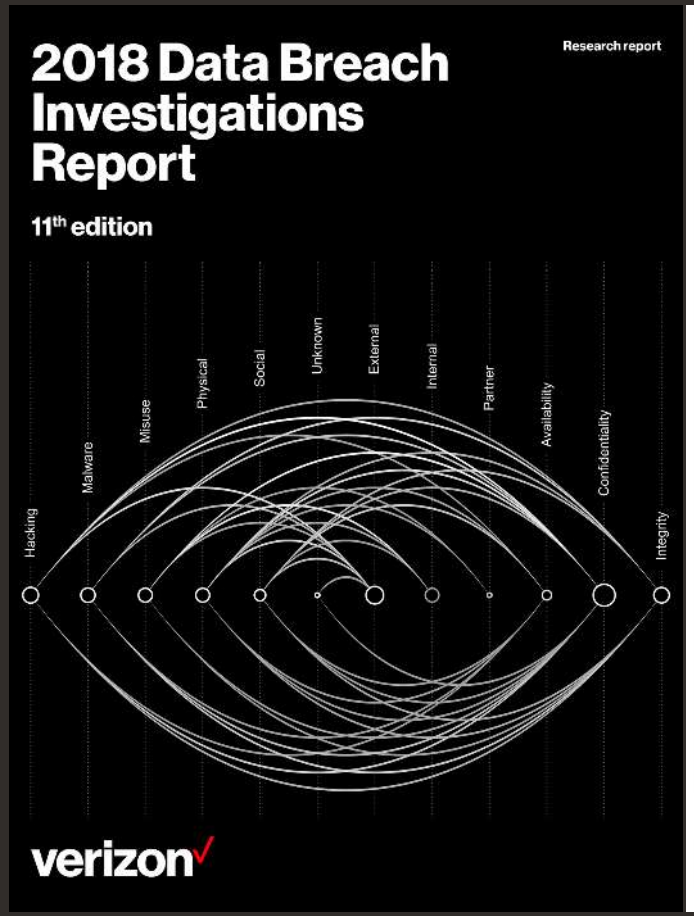
Информационная безопасность

Конфиденциальность,
Обеспечение доступа к информации только авторизованным пользователям

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

База данных - предпочтительная цель для атак



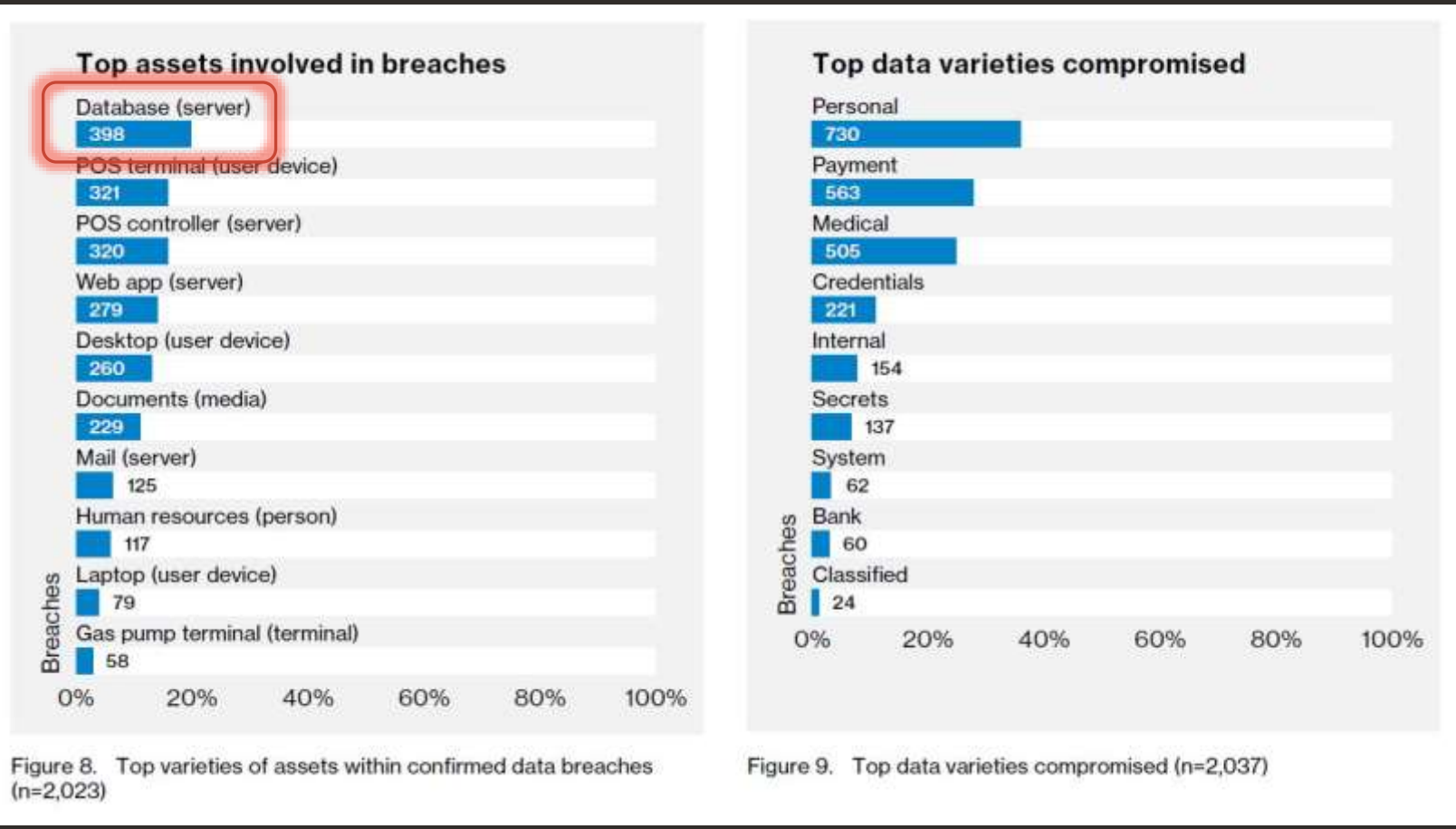


Figure 8. Top varieties of assets within confirmed data breaches (n=2,023)

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

База данных - предпочтительная цель для атак

2019 Data Breach Investigations Report

verizon business ready

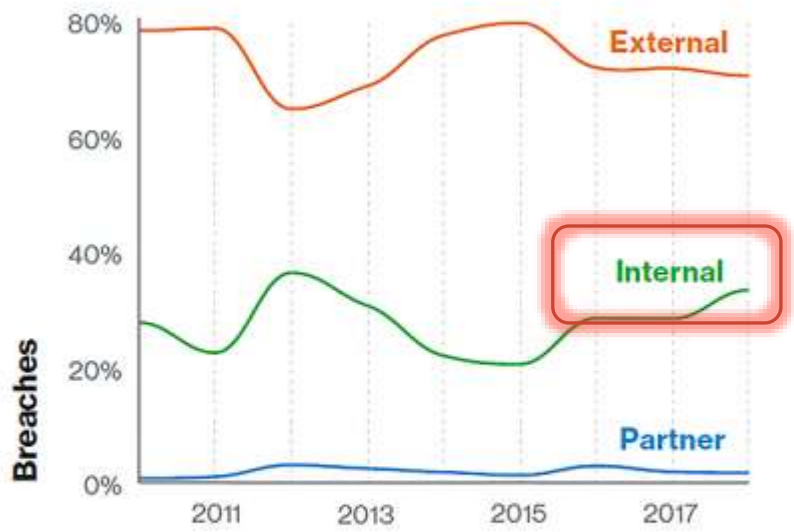


Figure 6. Threat actors in breaches over time

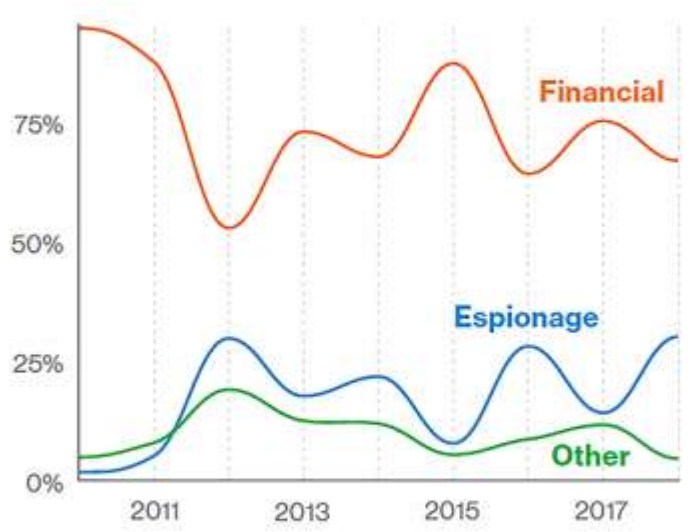
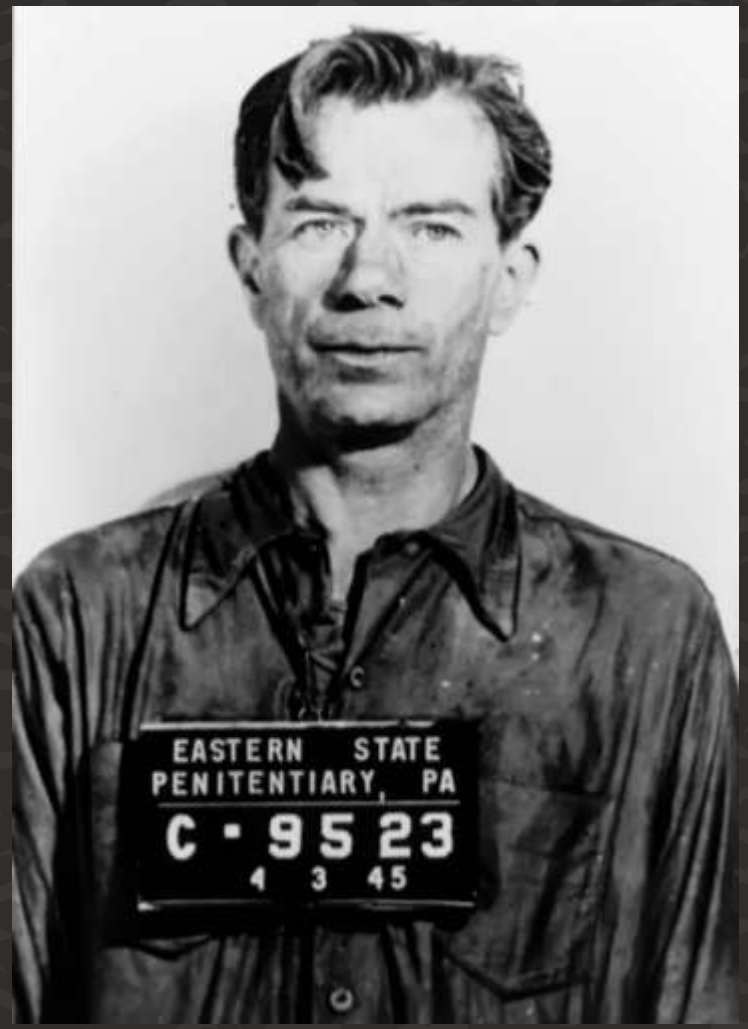


Figure 7. Threat actor motives in breaches over time

Willie "The Actor" Sutton 30.06.1901 — 02.11.1980

Грабитель, укравший на протяжении своей криминальной карьеры около двух миллионов долларов…
За свою жизнь ограбил более 100 банков.
На вопрос журналиста о том, почему он грабил банки, дал ответ «Потому что деньги были именно там»



Администратор базы данных Oracle

“…похитил более €600 тыс. … был признан виновным в совершении преступления, предусмотренного
ст.159 ч.4 УК РФ (мошенничество, т. е. хищение имущества в особо крупном размере), и ему было назначено наказание в виде 7 лет лишения свободы в колонии общего режима”

https://www.kommersant.ru/doc/1098330

Утечки данных в России

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

Технологии и медиа, 15 октября 2020, 17:00

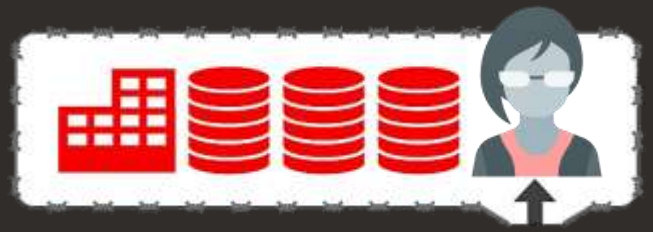
Более 90% компаний из России столкнулись с утечками данных

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

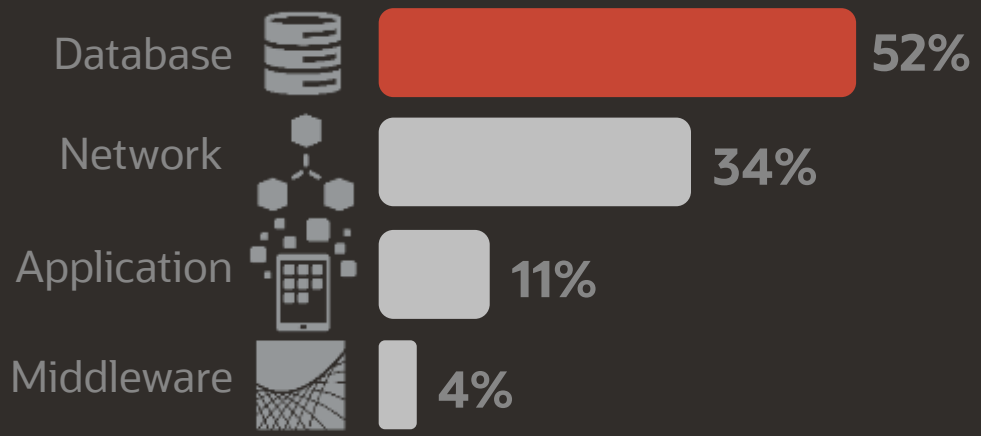
Фото: Angel Garcia / Bloomberg

База данных - предпочтительная цель для атак

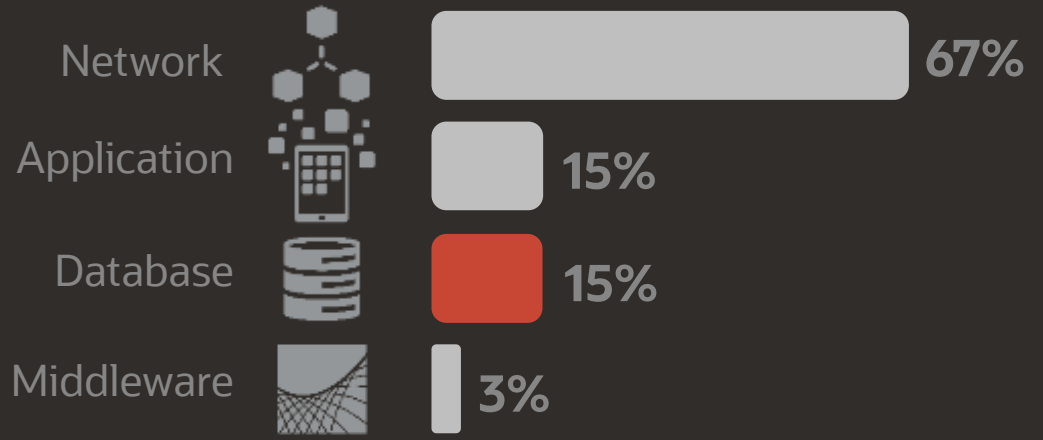
Защита с использованием "периметра ИБ"



Оценка уязвимости элементов IT



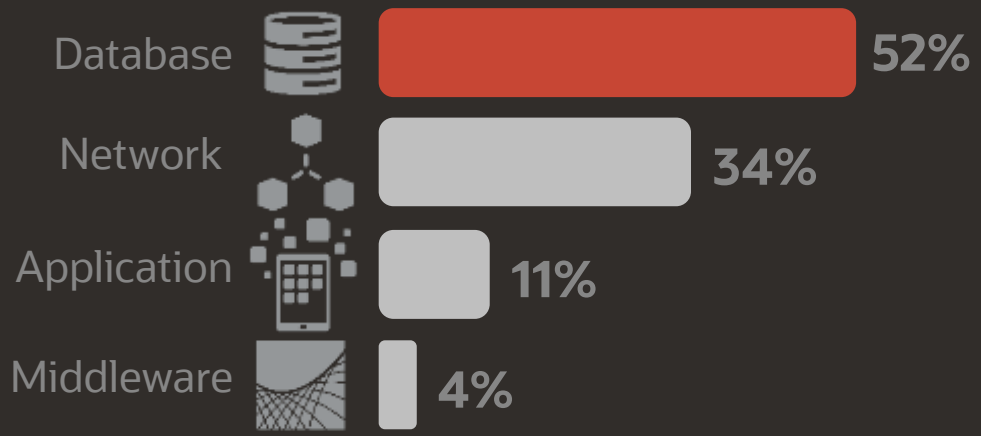
Затраты на противодействие утечкам



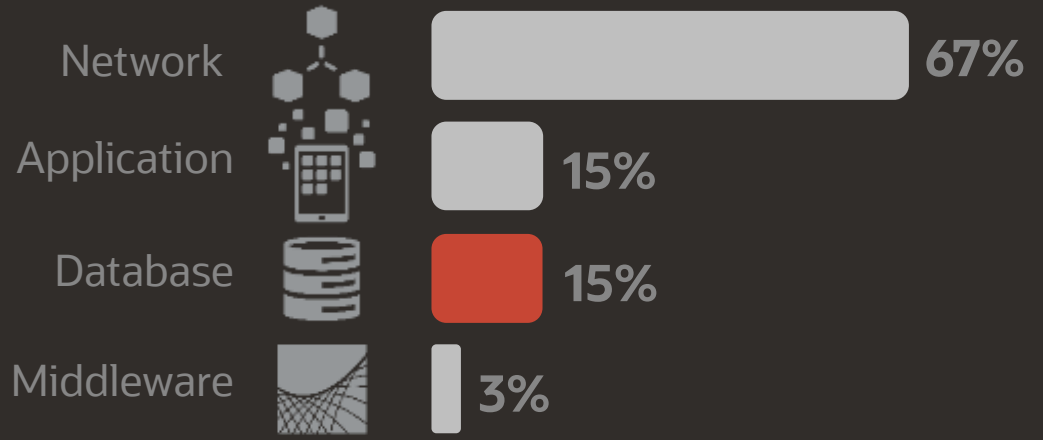
База данных - предпочтительная цель для атак

Требуется защита не только периметра, но и внутренней инфраструктуры

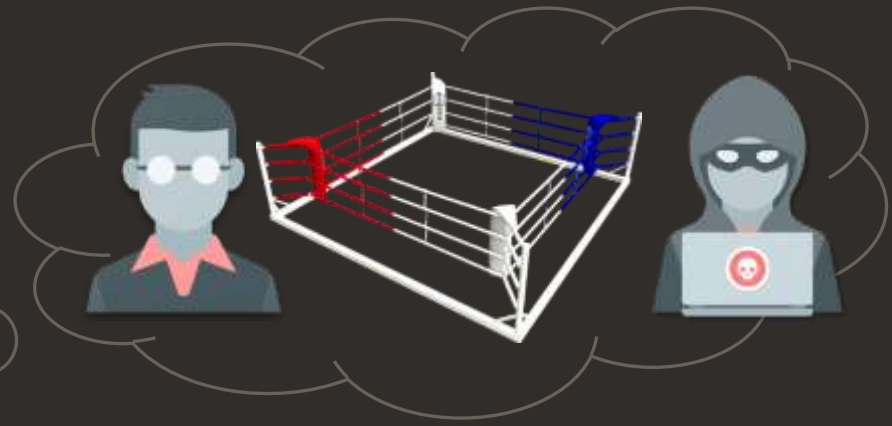
Оценка уязвимости элементов IT



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

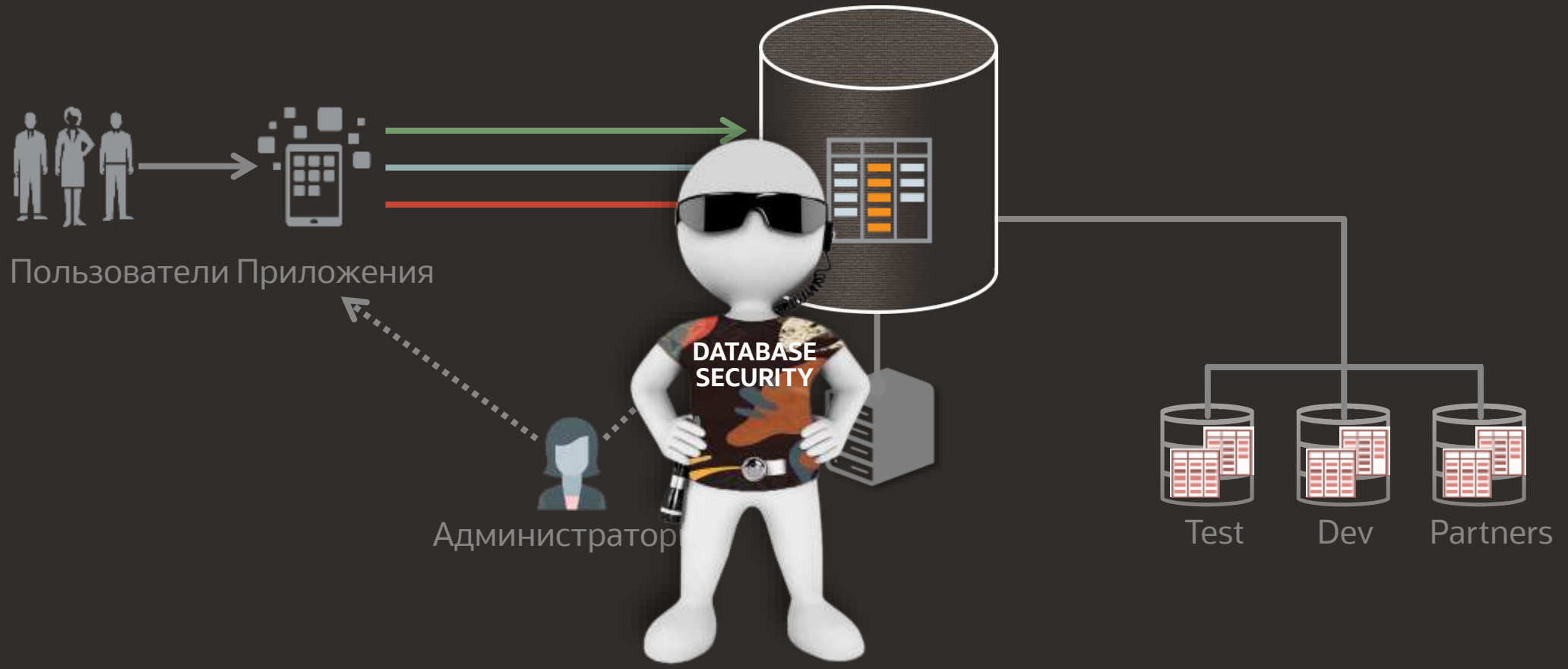
Претендент (злоумышленник)

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

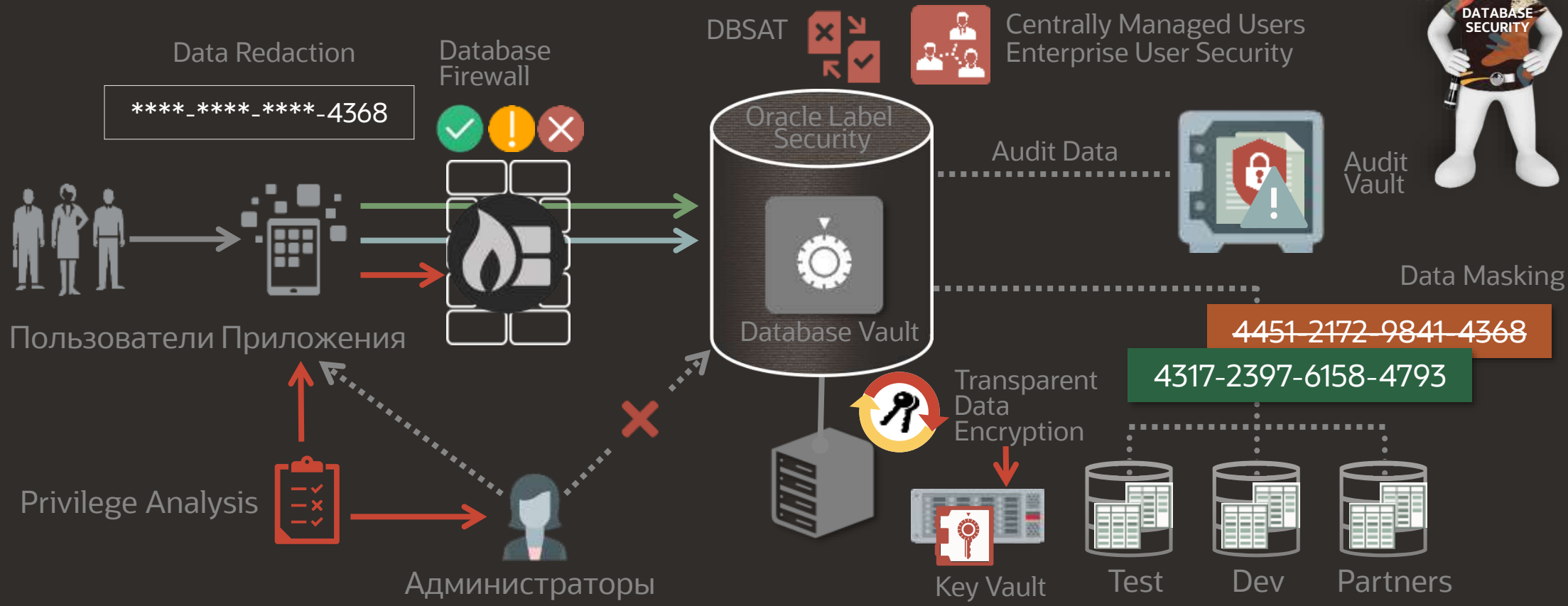
Защитник (невнимательный и наивный)

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

Как хакеры атакуют базы данных?



Oracle Database Maximum Security Architecture



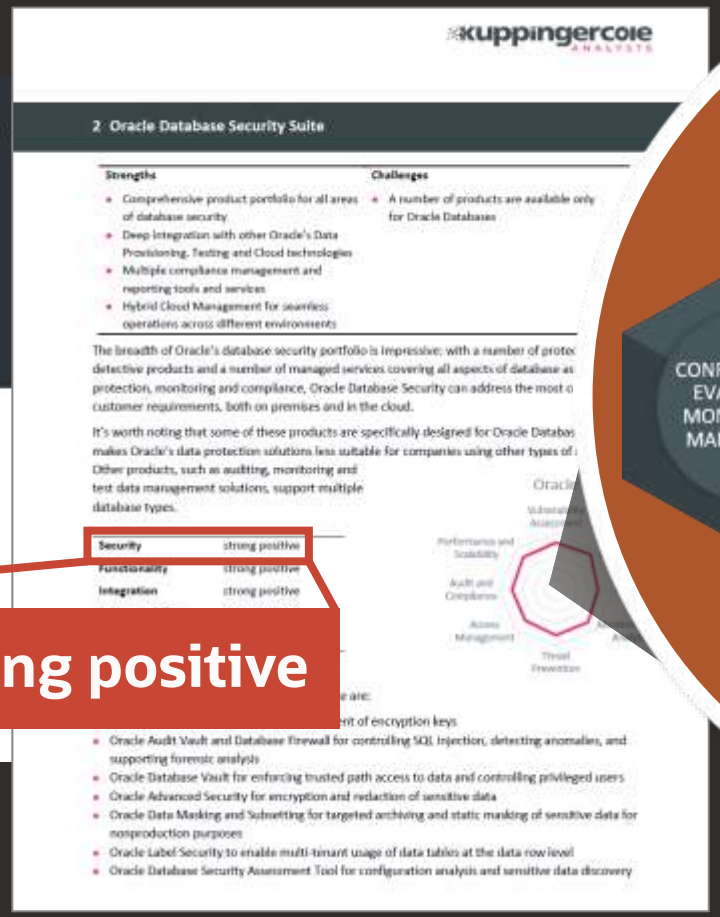
Средства защиты информации баз данных Oracle

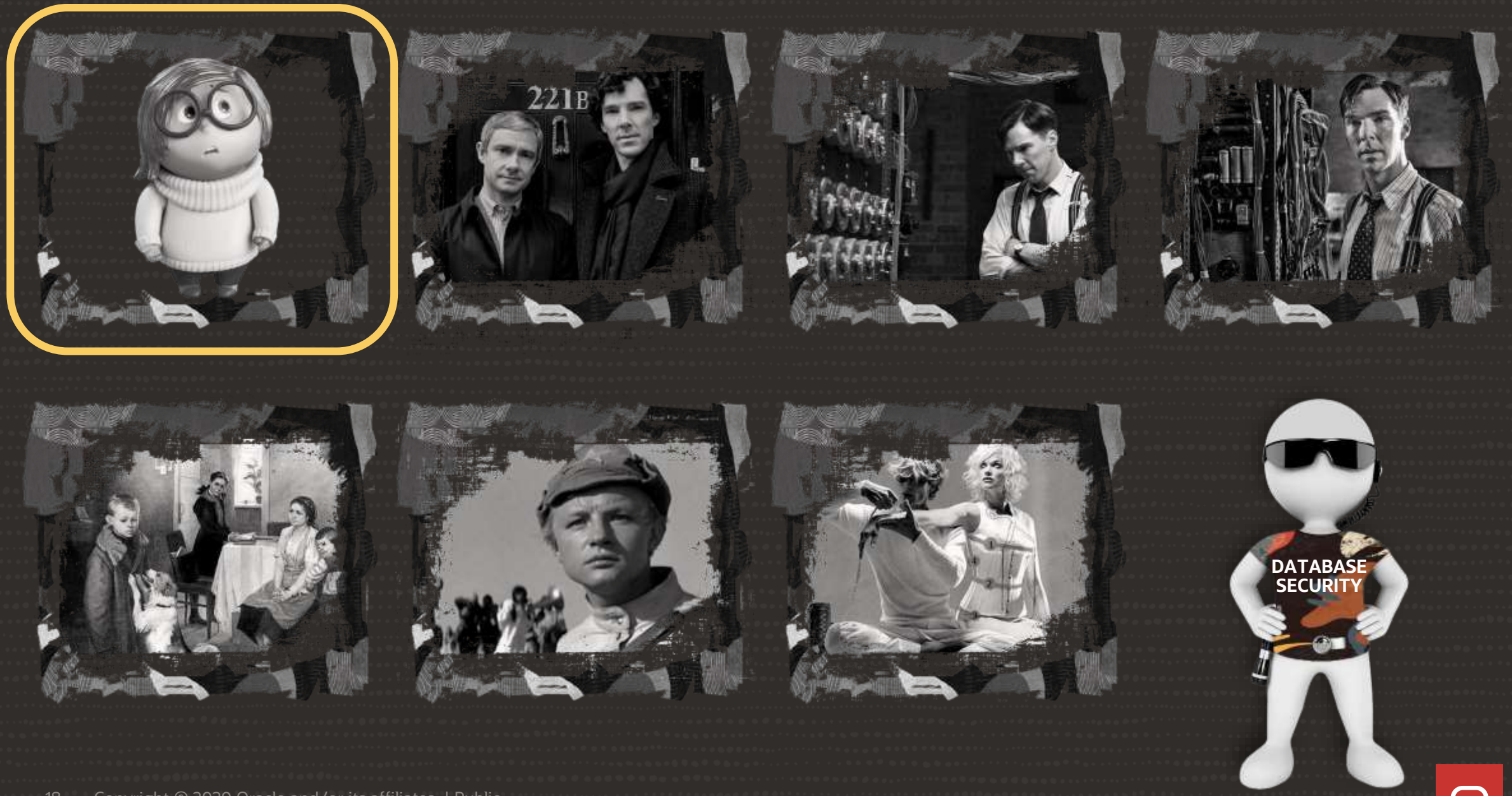
Мнение конкурентов

Базы данных, как и любые ИТ-системы, требуют специализированной защиты, и далеко не всегда лучшим решением являются штатные разработки производителей СУБД.
Для производства самих СУБД и систем их защиты применяются совершенно разные технологии, требующие наличия у разработчиков различных компетенций.

Средства защиты информации баз данных Oracle

Мнение экспертов





Database Security Assessment Tool (DBSAT)

Oracle Database Security Assessment Tool

Оценить уровень безопасности до того, как это сделают хакеры

Понять реальный уровень безопасности вашей БД

- Отчет об общем состоянии безопасности
- Поиск пользователей, оценка их прав и рисков
- Обнаружение конфиденциальных данных

Отчеты

- Обзорные и детальные
- Рекомендации для устранения замечаний
- Mapping to EU GDPR and CIS Benchmark

Анализ для Oracle Database 10g (10.2.0.5, 11g, 12c, 18c и 19c)

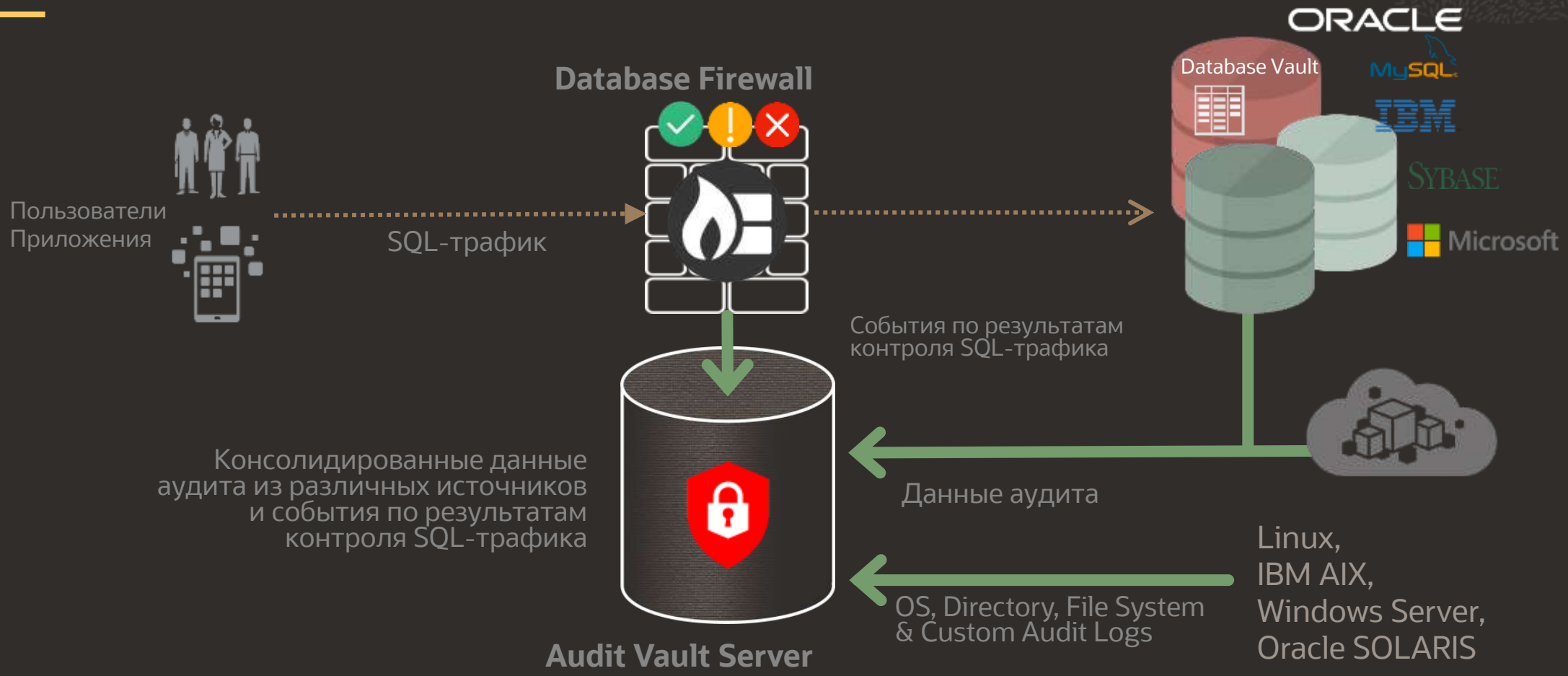
Автономный инструмент: быстрый, легкий

Бесплатно для текущих пользователей Oracle

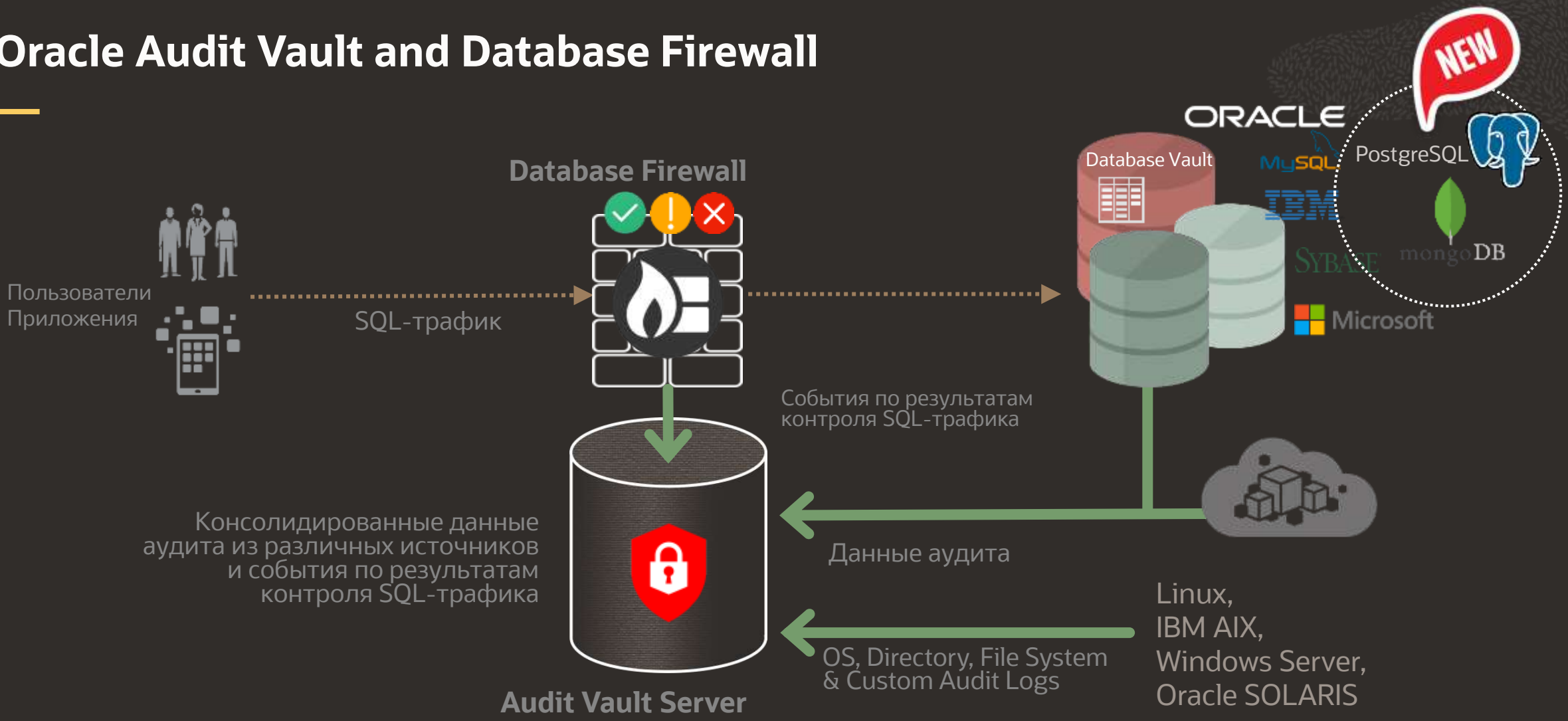
DBSAT

Audit Vault and Database Firewall (AVDF)

Oracle Audit Vault and Database Firewall

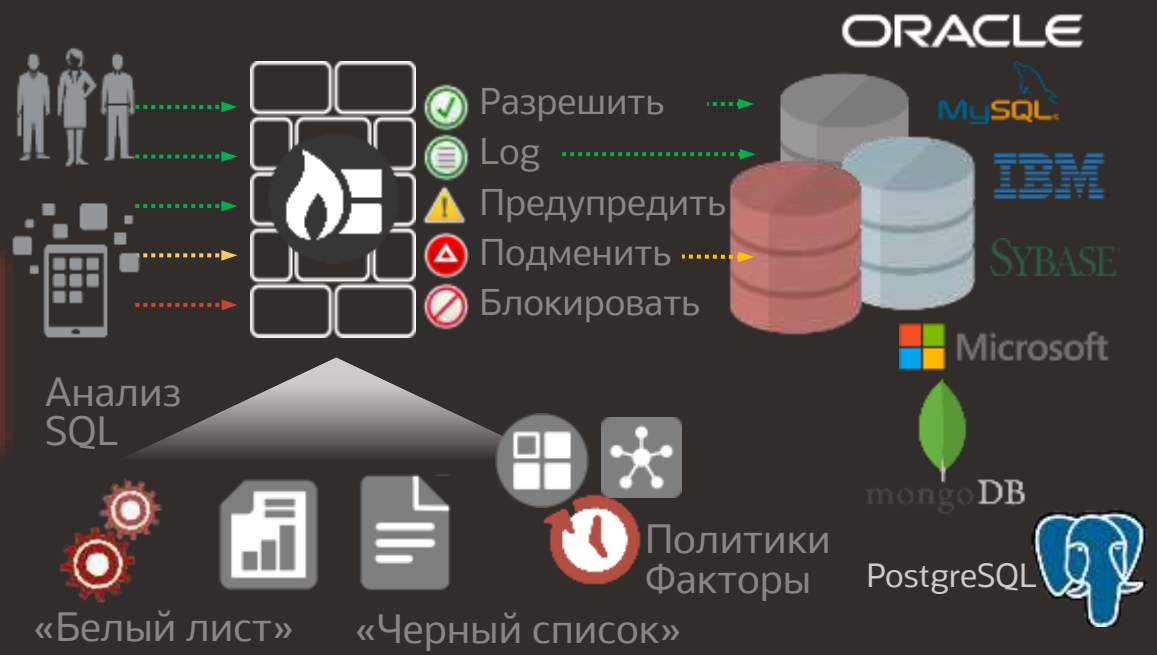


Oracle Audit Vault and Database Firewall



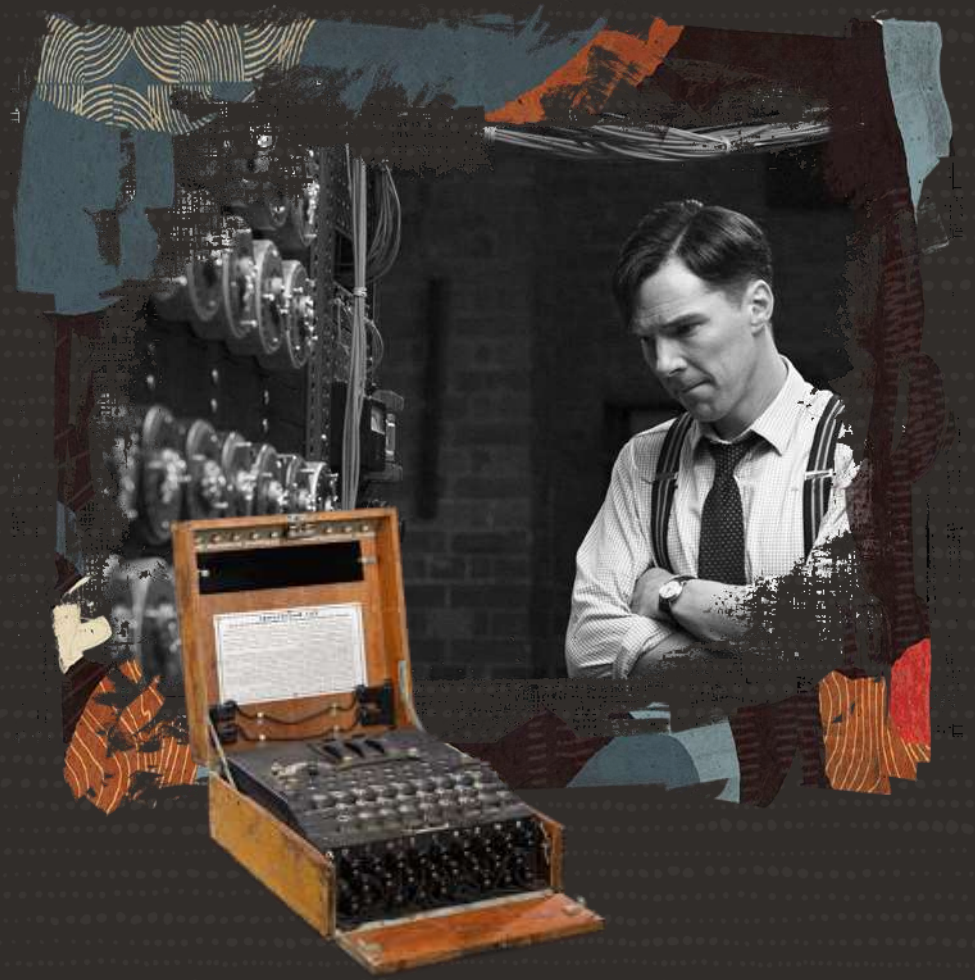
Database Firewall : Контроль SQL-трафика

- Мониторинг трафика и исключение неавторизованного доступа к базам данных, исключение SQL инъекций, позволяющих не санкционировано повышать привилегии и получать доступ к конфиденциальным данным.
- Аккуратный грамматический анализ SQL выражений
- Высокая масштабируемость и производительность
- Встроенные отчеты для анализа соответствия нормативным требованиям



DBSAT

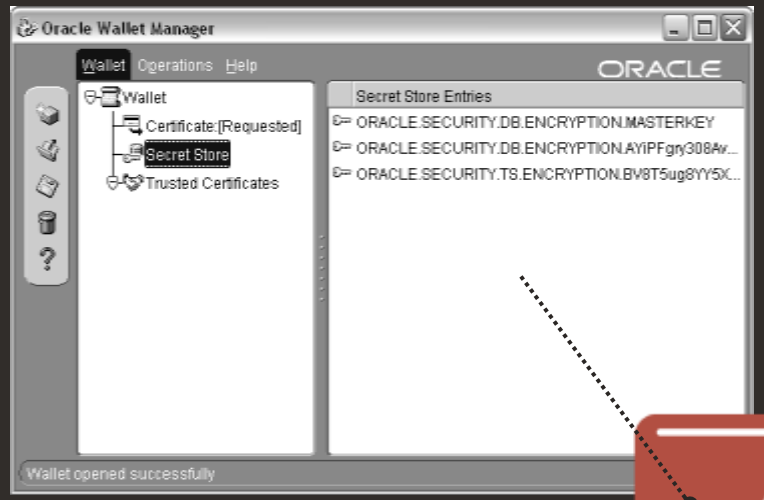
AVDF



Advanced Security Options (ASO)

Advanced Security Options

Шифрование данных



Password

Данные зашифрованы

(…3DES168, AES128-256, ARIA128-256, GOST256)

Защищенный формат хранения

Root *

Злоумышленник, имеющий высокий уровень привилегий в ОС

Personal, Payment, Medical, Credentials, Internal, Secrets, System, Bank, Classified

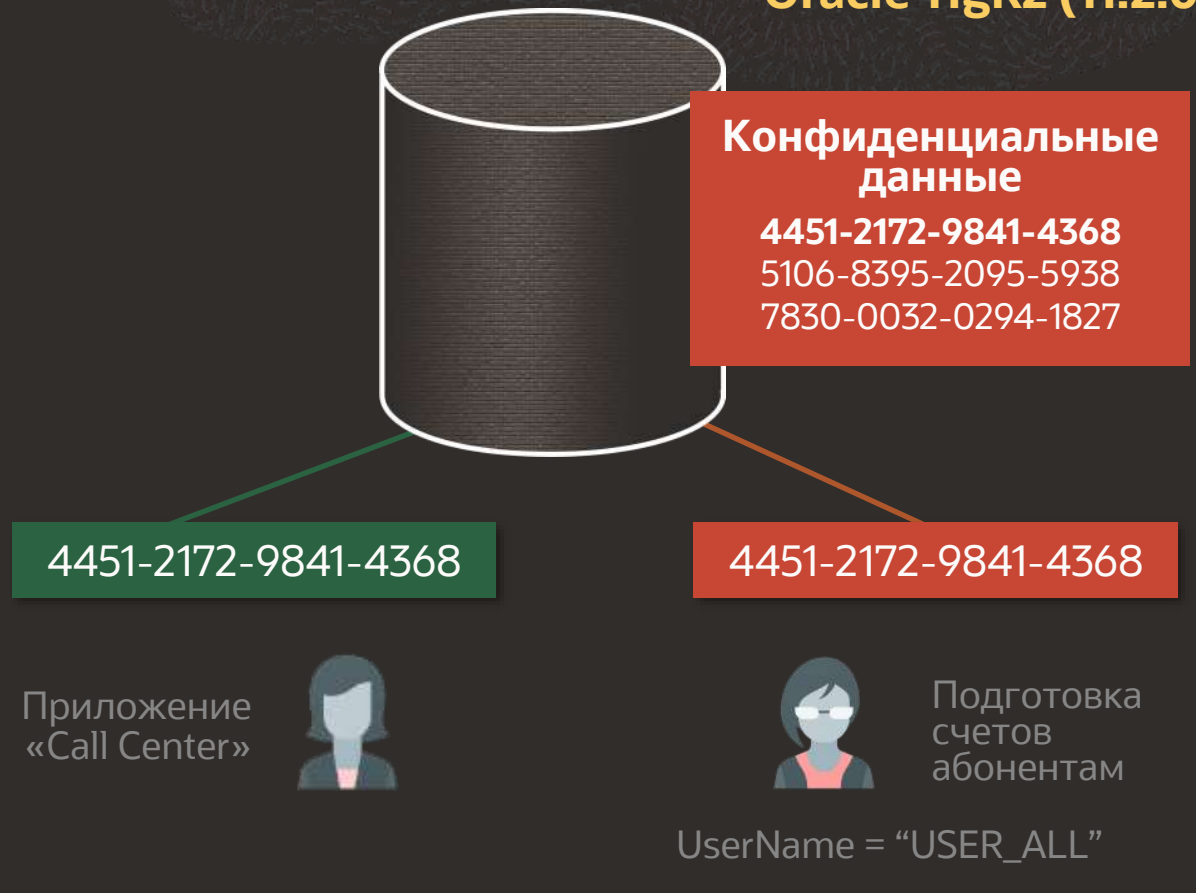
Обычный формат хранения

Advanced Security Options

Data Redaction

- Изменение способа отображения конфиденциальных данных с учетом контекста (имя пользователя, IP-адрес…)
- Библиотека политик для быстрой настройки отображений
- «Прозрачно» для приложений и пользователей

Oracle 11gR2 (11.2.0.4)



Advanced Security Options

Data Redaction / Как и зачем проводить динамическое маскирование?

Задачи

- Дополнительная защита при отображении конфиденциальных данных на пользовательских устройствах
- Выполнение регулятивных требований по защите информации от несанкционированного доступа
- Минимальные потребные изменения в базе данных и приложениях

Способы

- **Full**
  - 10/09/2012 -> 01/01/2001
- **Partial**
  - 4451-2172-9841-4368 -> ****-****-****-4368
- **Regular Expression**
  - first.last@eg.com -> [hidden].last@eg.com
- **Random**
  - 8914578940 -> 3678904532

Advanced Security Options

Data Redaction / Политика «COS_REDACTION»

```
BEGIN
  DBMS_REDACT.add_policy (object_schema => 'ANYBANK'
   , object_name          => 'COS'
   , policy_name          => 'COS_REDACTION'
   , expression           => 'SYS_CONTEXT(''USERENV'',''SESSION_USER'') != ''USER_ALL'''
   , column_name          => 'GEO'
   , function_type        =>  DBMS_REDACT.RANDOM
   );

  DBMS_REDACT.ALTER_POLICY(object_schema => 'ANYBANK'
   , object_name          => 'COS'
   , policy_name          => 'COS_REDACTION'
   , action               => DBMS_REDACT.ADD_COLUMN
   , column_name          => 'LEGAL_NAME'
   , function_type        => DBMS_REDACT.RANDOM
    );

DBMS_REDACT.ALTER_POLICY(object_schema => 'ANYBANK'
   , object_name          => 'COS'
   , policy_name          => 'COS_REDACTION'
   , action               => DBMS_REDACT.ADD_COLUMN
   , column_name          => 'CREDIT_CARD_NUM'
   , function_type        => DBMS_REDACT.PARTIAL
   , function_parameters => 'VVVVFVVVVFVVVVFVVV,VVVV-VVVV-VVVV-VVVV,*,1,12'
    );
END;
/
```

Random

Partial

ORACLE DATABASE 12c

Oracle 11gR2 (11.2.0.4)

Конфиденциальные данные

4451-2172-9841-4368
5106-8395-2095-5938
7830-0032-0294-1827

Redaction Policy

****-****-****-4368

4451-2172-9841-4368

Приложение «Call Center»

Подготовка счетов абонентам

UserName = “USER_ALL”

Advanced Security Options

Редакция отображаемых данных и шифрование

ORACLE DATABASE 12c

Oracle 11gR2 (11.2.0.4)

Wallet

Data Redaction

****-****-****-5100

Redacted Applications

Конфиденциальные данные

4451-2172-9841-5100

5106-8395-2095-5938

7830-0032-0294-1827

Transparent Data Encryption

Encrypted Storage

d$f8#;!90Wz@Yg#3

DBSAT

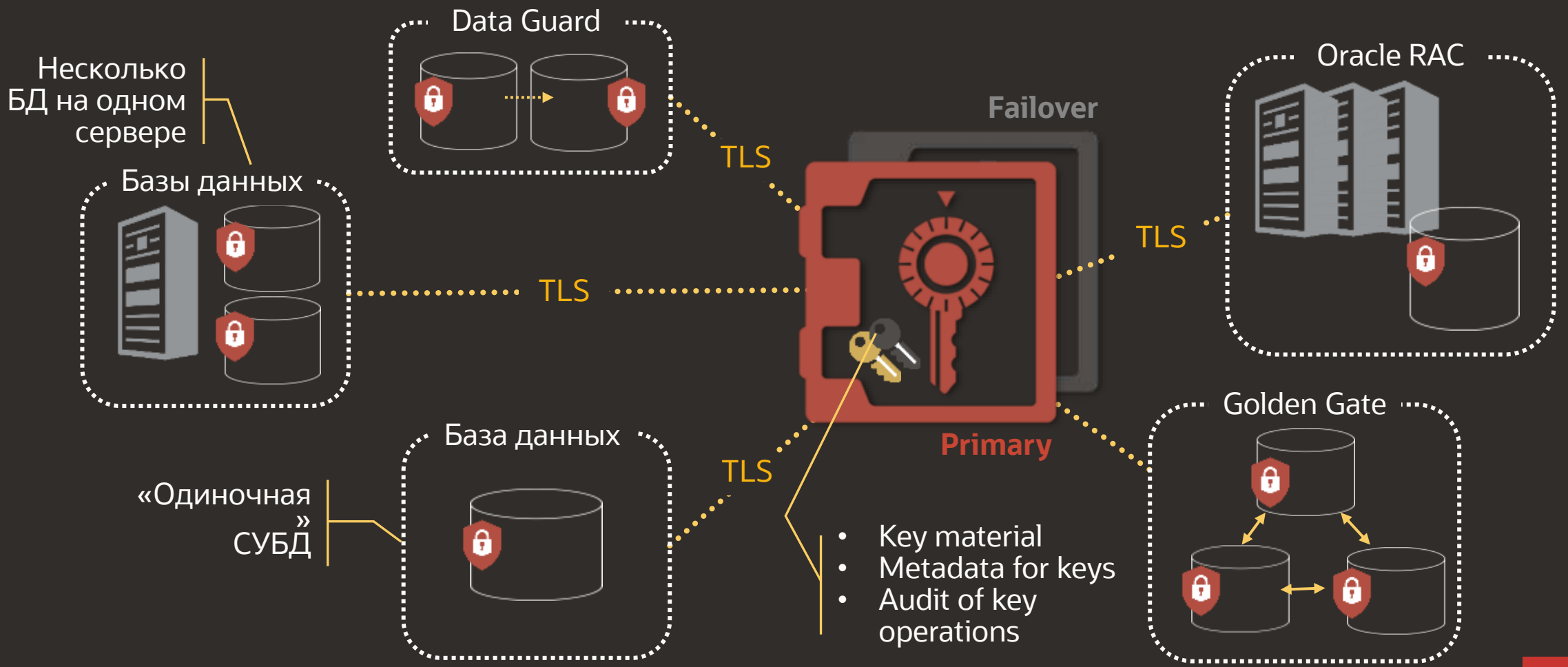
AVDF

ASO

Oracle Key Vault (OKV)

Oracle Key Vault

Централизованное управление мастер-ключами TDE / онлайн-мастер-ключ



Oracle Key Vault

Сохранение данных WALLET в OKV

/etc/ORACLE/WALLETS/oracle

CUSTOMER_DB_WALLET

WALLET

```
./okvutil upload -t WALLET -l /etc/ORACLE/WALLETS/oracle -g CUSTOMER_DB_WALLET
```

Oracle Key Vault

WALLET не открылся (испорчен файл) ?

/etc/ORACLE/WALLETS/oracle

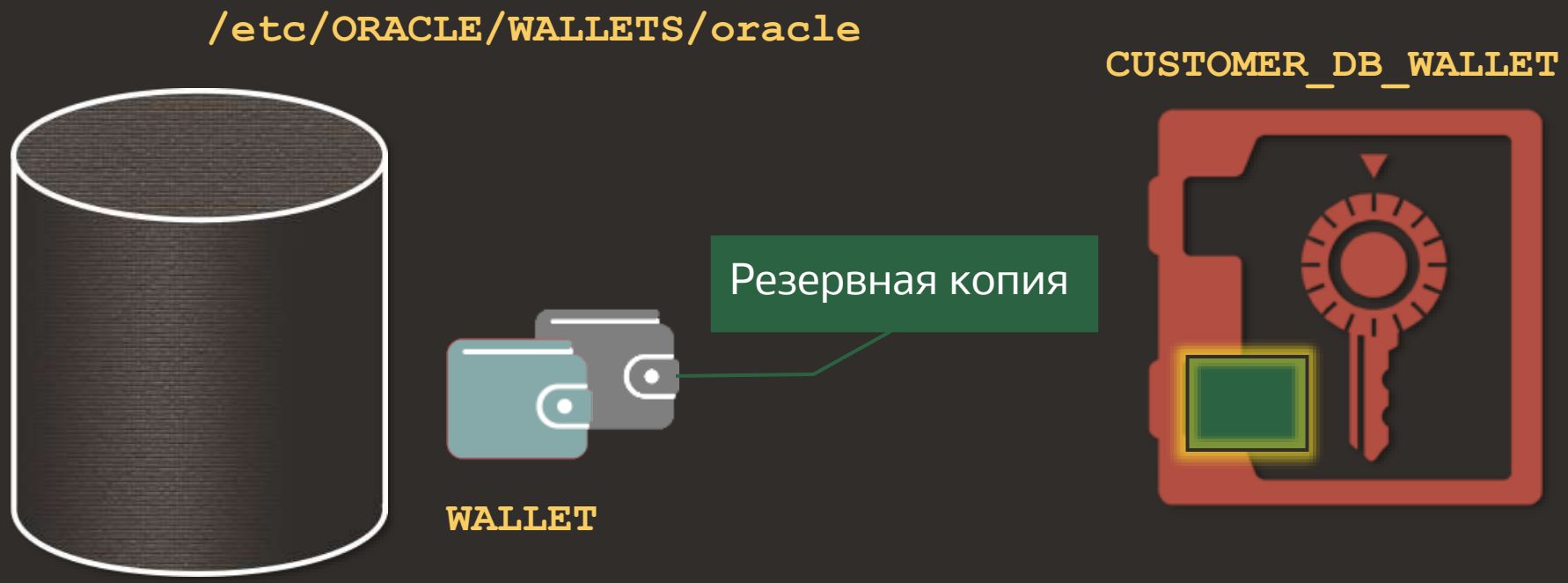
WALLET

```
SQL> startup
ORACLE instance started.

Total System Global Area  801701888 bytes
Fixed Size                  2257520 bytes
Variable Size             272633232 bytes
Database Buffers          520093696 bytes
Redo Buffers                6717440 bytes
Database mounted.
ORA-28365: wallet is not open
```

Oracle Key Vault

Восстановление WALLET из OKV




```
./okvutil download -t WALLET -l /etc/ORACLE/WALLETS/oracle -g CUSTOMER_DB_WALLET
```

```
NEW WALLET PASSWORD: ******
```

DBSAT

AVDF

ASO

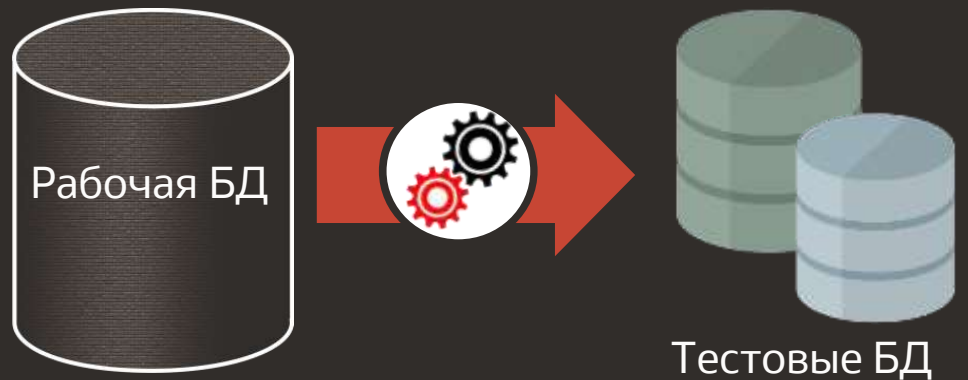
Key Vault

Masking and Subsetting Pack

Маскирование данных (статическое) для задач тестирования

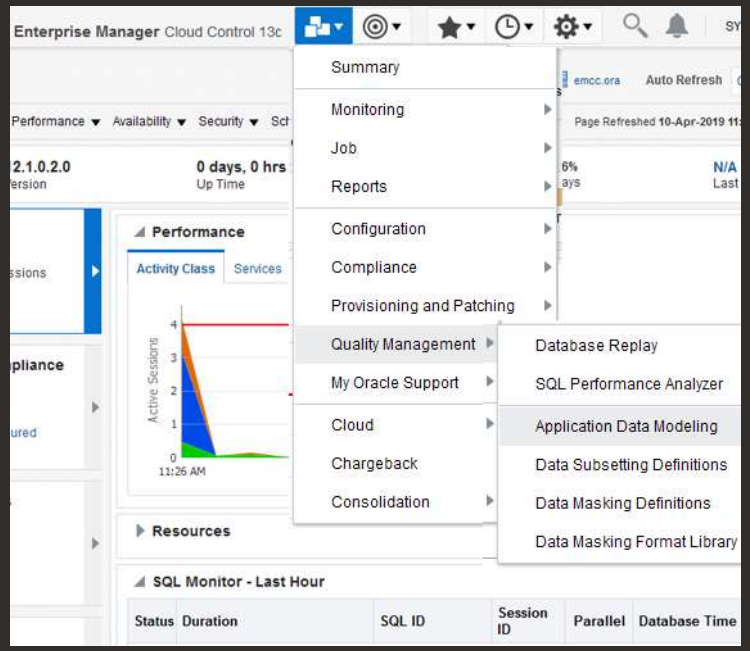
- Подмена конфиденциальных данных приложений
- Ссылочная целостность данных
- Расширяемая библиотека шаблонов и форматов
- Специализированные шаблоны для приложений
- Поддержка маскирования данных в БД сторонних производителей

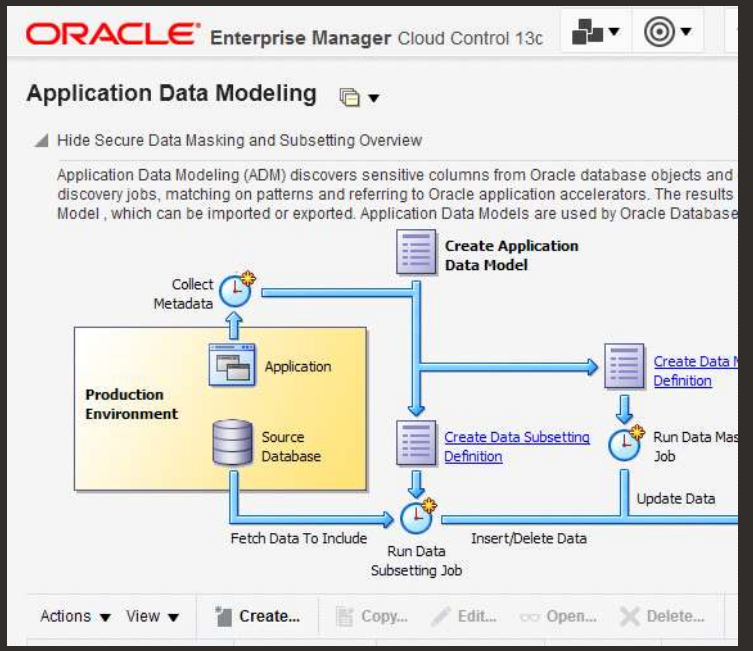
LAST_NAME	SSN	SALARY
AGUILAR	203-33-3234	40,000
BENSON	323-22-2943	60,000



LAST_NAME	SSN	SALARY
ANSKEKSL	323-23-1111	60,000
BKJHHEIEDK	252-34-1345	40,000

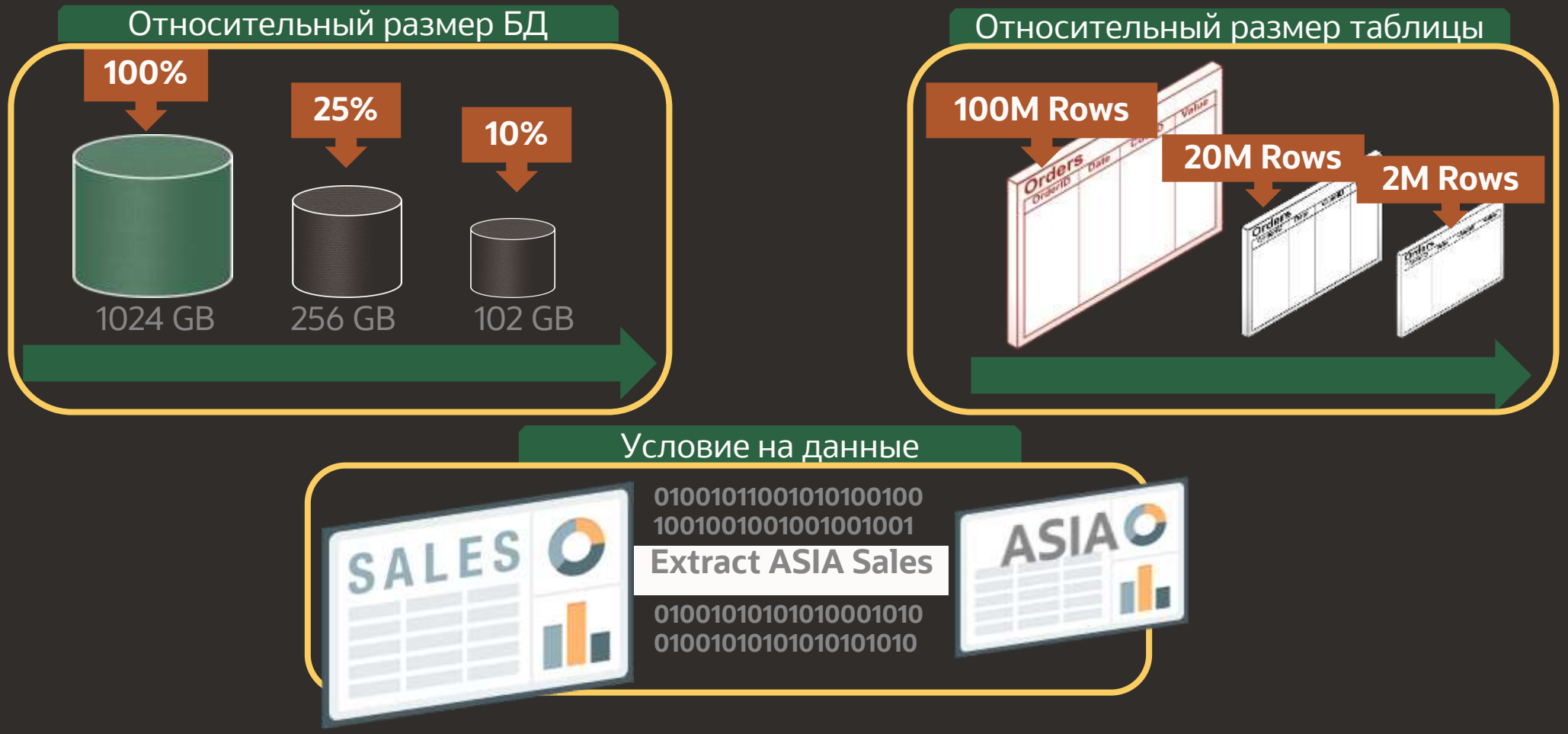
Oracle Data Masking and Subsetting Pack





Оценка модели данных (**Application Data Modeling**) – первый этап маскирования данных

Урезание объема данных по условию



Урезание объема данных по условию

Оценка объема данных после урезания

Applications | Table Rules | Rule Parameters | **Space Estimates** | Pre/Post Subset Script

Impact of subset rules on tables are displayed below. The values shown here are based on estimates and may not be accurate.

View ▾ | Refresh...

Name	Table Rule	Source Size		Estimated Subset Size		
		MB	Rows	MB	Rows	%
▽ Applications and Tables		912.1908	8661245	483.5967	4438883	53.01
▽ TDM(TDM)		912.1908	8661245	483.5967	4438883	53.01
H_LINEITEM		606.6597	6001215	246.1027	2434504	40.57
H_ORDER	o_custkey in (select c_custkey from tdm.h_custo...	148.7732	1500000	88.6328	893637	59.58
H_PARTSUPP		109.1003	800000	109.1003	800000	100
H_CUSTOMER		24.0326	150000	16.1358	100712	67.14
H_PART		22.316	200000	22.316	200000	100
H_SUPPLIER		1.3065	10000	1.3065	10000	100
H_NATION		0.0021	25	0.0021	25	100
H_REGION		0.0004	5	0.0004	5	100

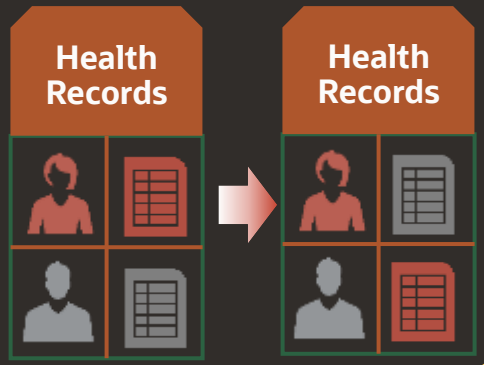
Различные варианты маскирования

Mask Based on Condition

Cntry	Identifier
CA	226-956-324
US	610-02-9191
UK	JX 75 67 44 C

Cntry	Identifier
CA	368-132-576
US	829-37-4729
UK	AI 80 56 31 D

Shuffle Records



Generate Deterministic Output

Emp ID	First Name
324	Albert
986	Hussain

HR

Emp ID	First Name
324	Charlie
986	Murali

FIN

Emp ID	First Name
324	Charlie
986	Murali

Generate Random Values Preserving Format

Company	Closing Price
IBFG	$36.92
XKJU	¥789.8

Company	Closing Price
IBFG	$89.57
XKJU	¥341.9

Mask Operating System Files stored as Blobs

BLOB
3178973456
6509876745

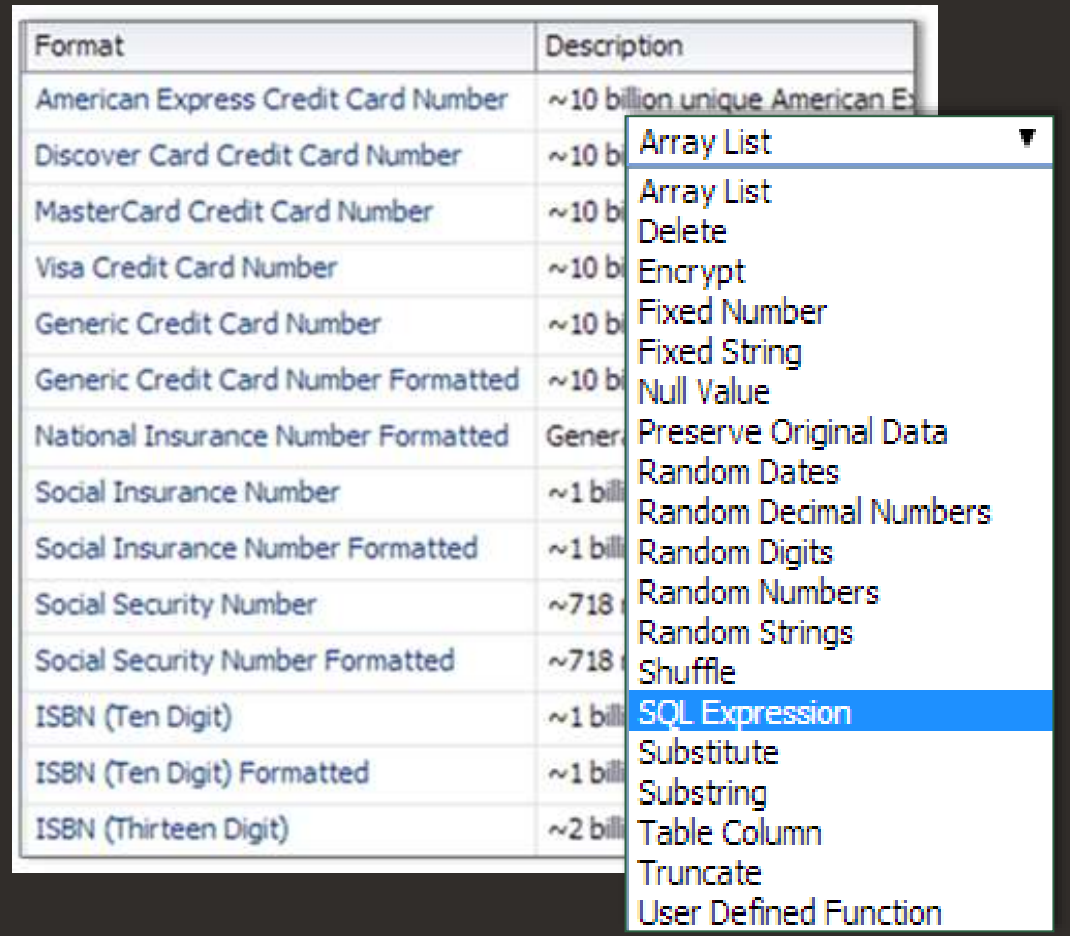
Search : [0-9]{10}
Replace : *

BLOB
****
****

и другие…

Обширная библиотека форматов

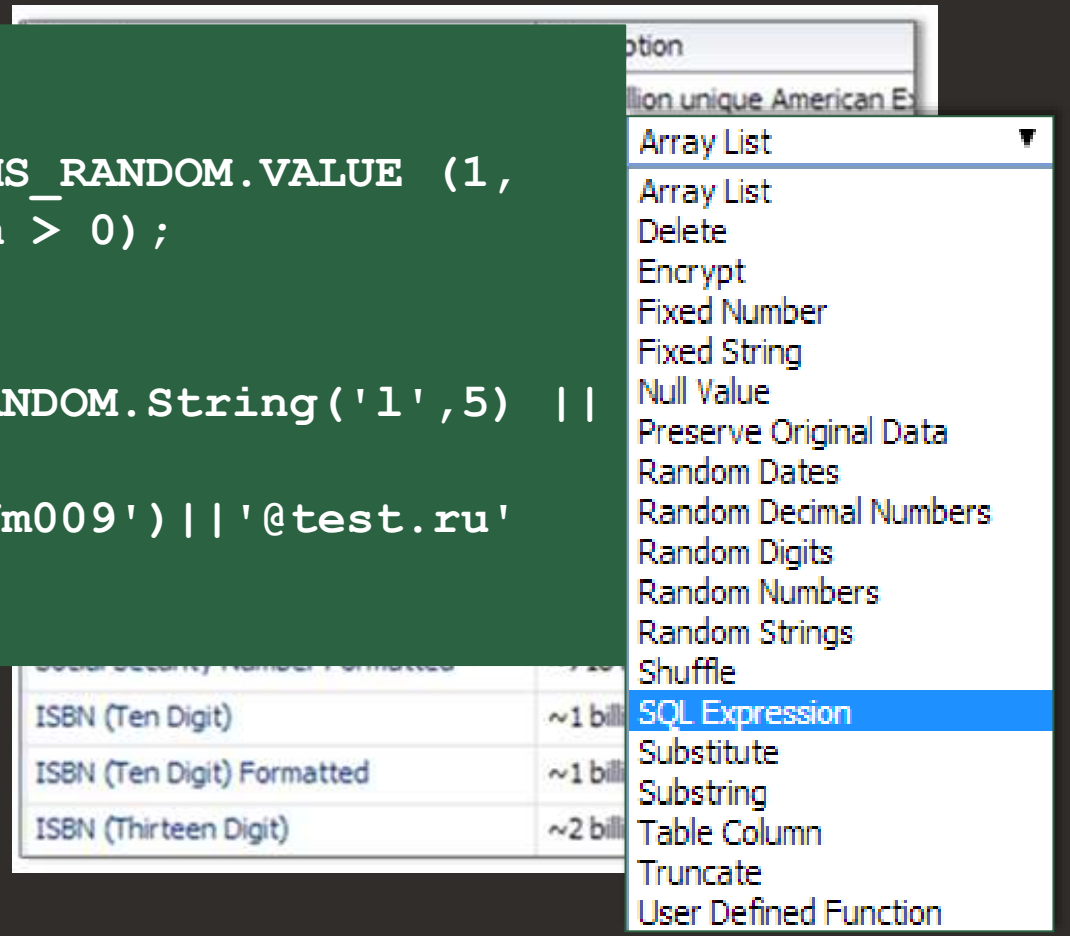
- Содержит основные форматы маскирования
- Обеспечивает поддержку пользовательских форматов
  - Random numbers/strings/dates
  - Substitute
  - User defined PL/SQL function
  - … и другие
- Шаблоны для E-Business Suite и Fusion Applications



Обширная библиотека форматов

```
-- Случайная дата
select * from (select to_char(sysdate - DBMS_RANDOM.VALUE (1,
18250),'DD/MM/YYYY') from dual where rownum > 0);

-- eMail
select DBMS_RANDOM.String('u',1) || DBMS_RANDOM.String('l',5) ||
'_' ||
to_char(mod(dbms_random.value*10E37,999),'fm009')||'@test.ru'
from dual;
```



Способы организации процесса маскирования

In-Database

Минимальная дополнительная нагрузка
на сервер базы данных источника

Разнородные источники

In-Export

Oracle

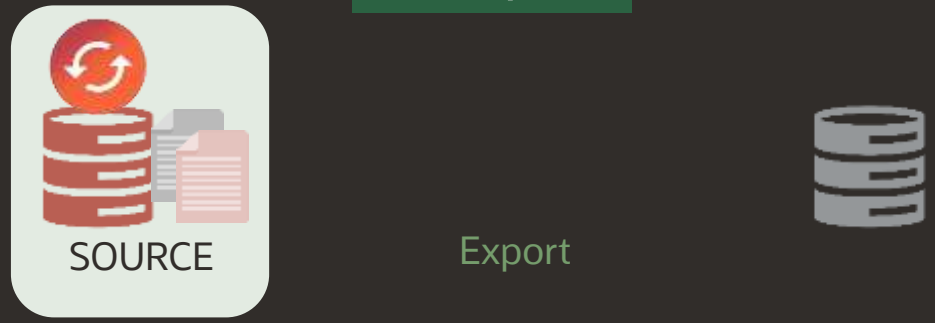
Способы организации процесса маскирования

In-Database

Минимальная дополнительная нагрузка
на сервер базы данных источника

Разнородные источники

In-Export



Проще обеспечить защищенность
(не требуется расширять доверенное окружение)

Oracle

DBSAT

AVDF

ASO

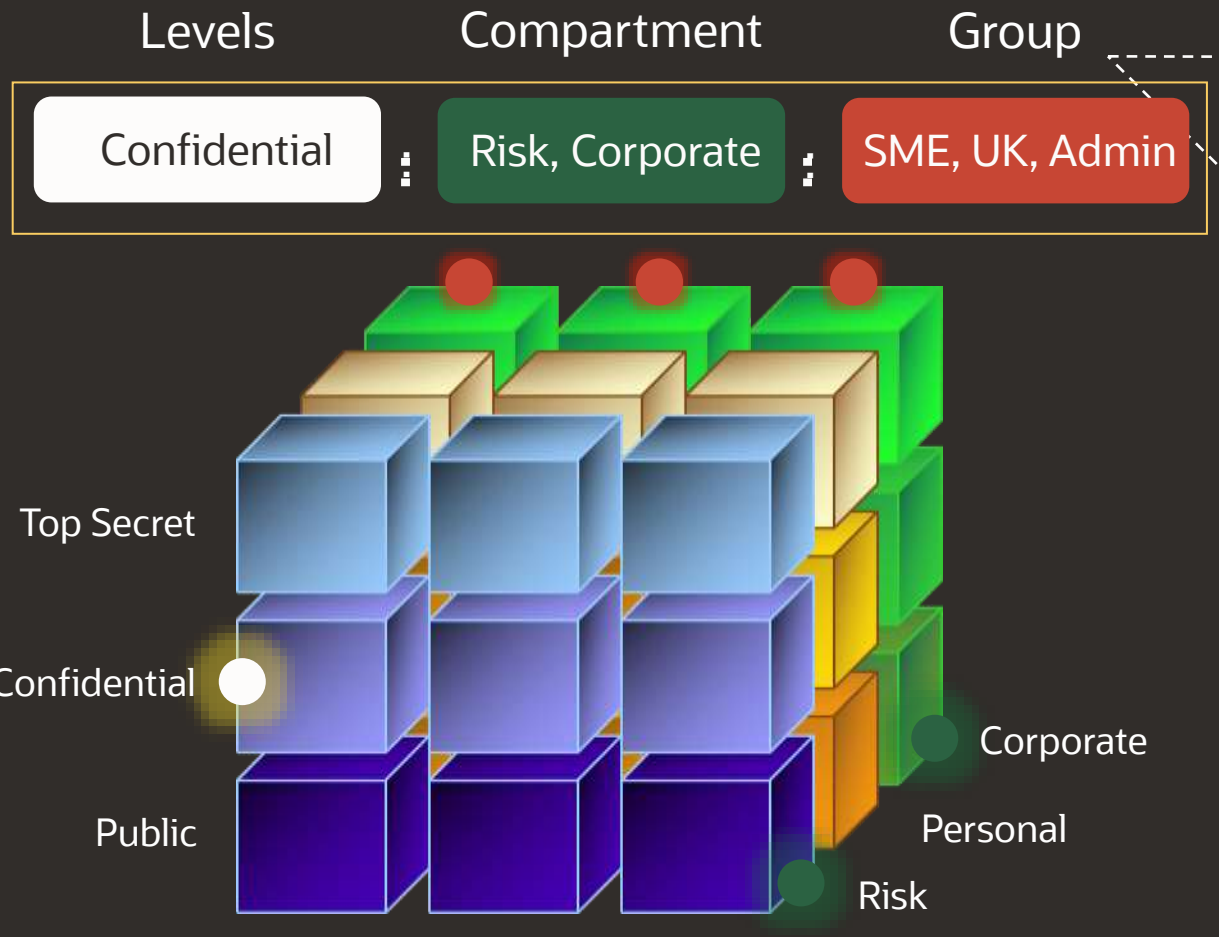
Key Vault

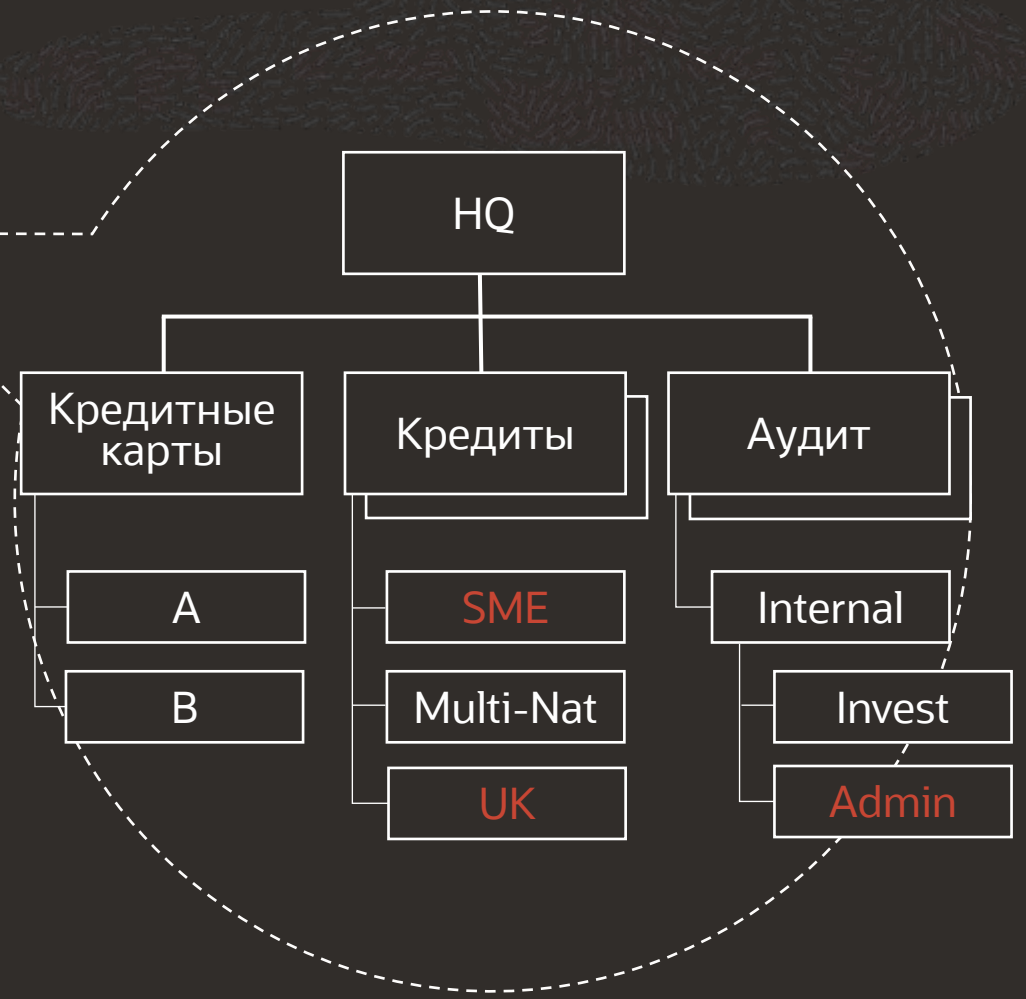
Masking Pack

Oracle Label Security (OLS)

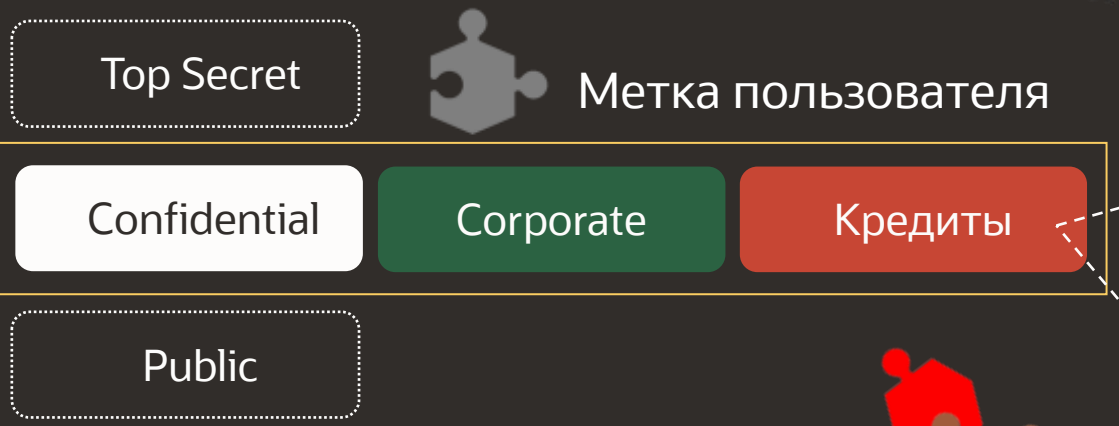
Oracle Label Security

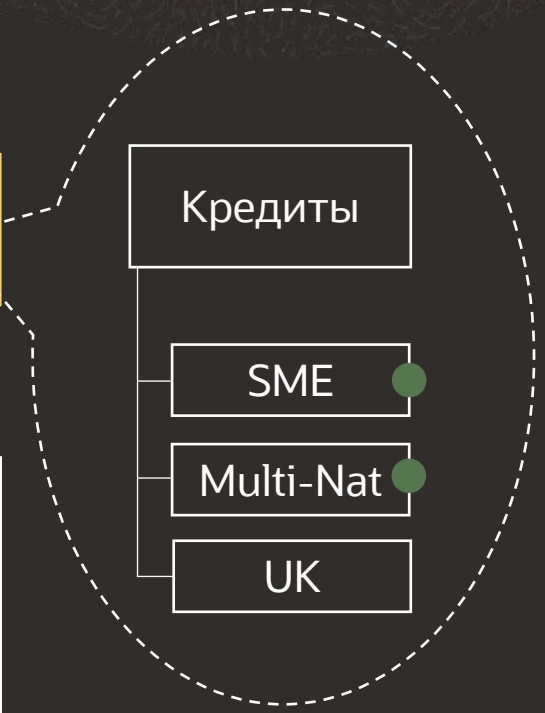
Пример метки





Oracle Label Security
Пример чтения данных





Код	Количество	Метка строки
AF2137	100000	Confidential : Corporate : SME
JG4112	225000	Confidential : Personal : London
XS302	575000	Top Secret : Risk : Audit
AF2991	317000	Public : Personal : Branch
SD1328	900725	Public : Corporate: Multi-Nat

DBSAT

AVDF

ASO

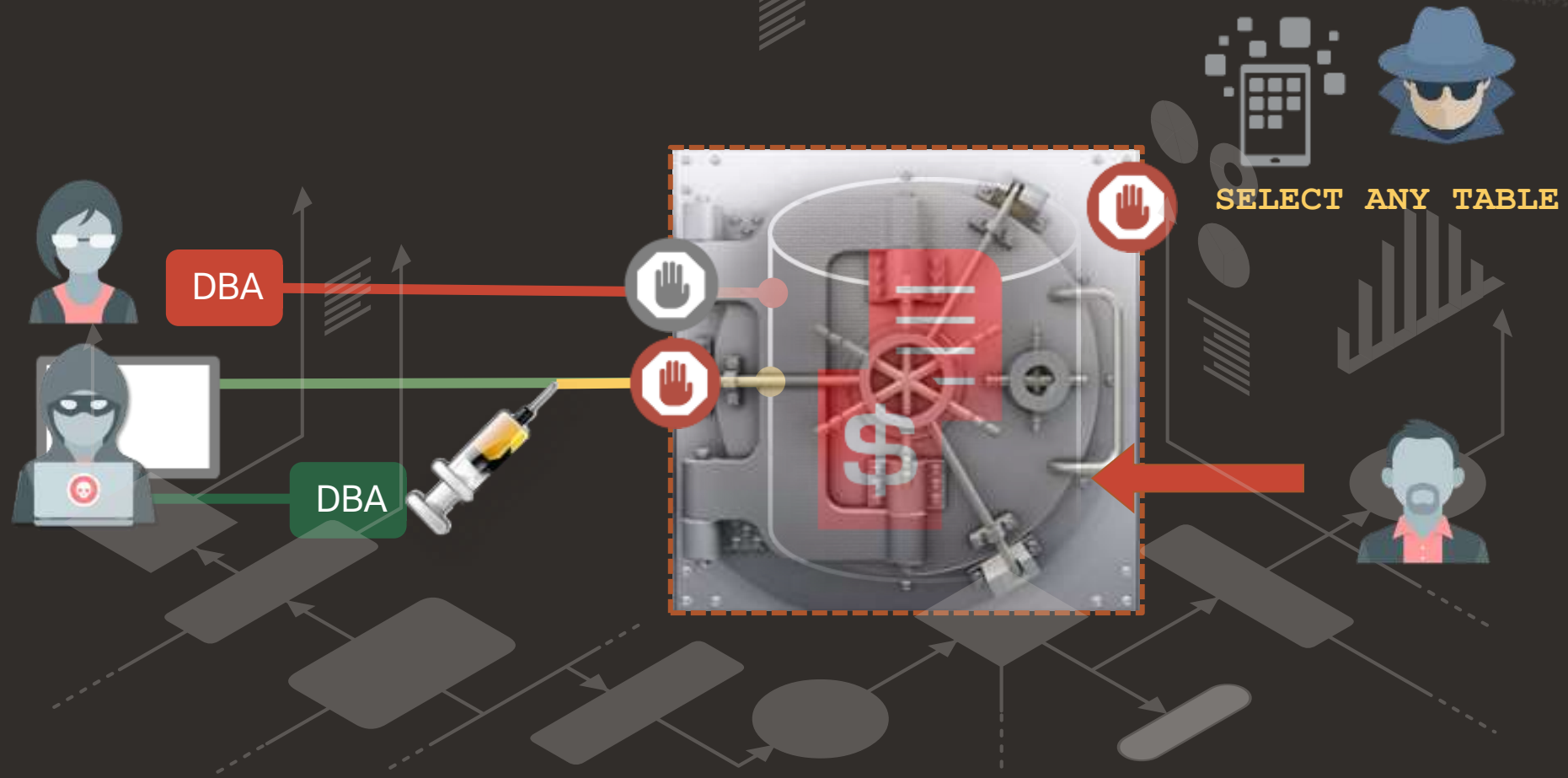
Key Vault

Masking Pack

Label Security

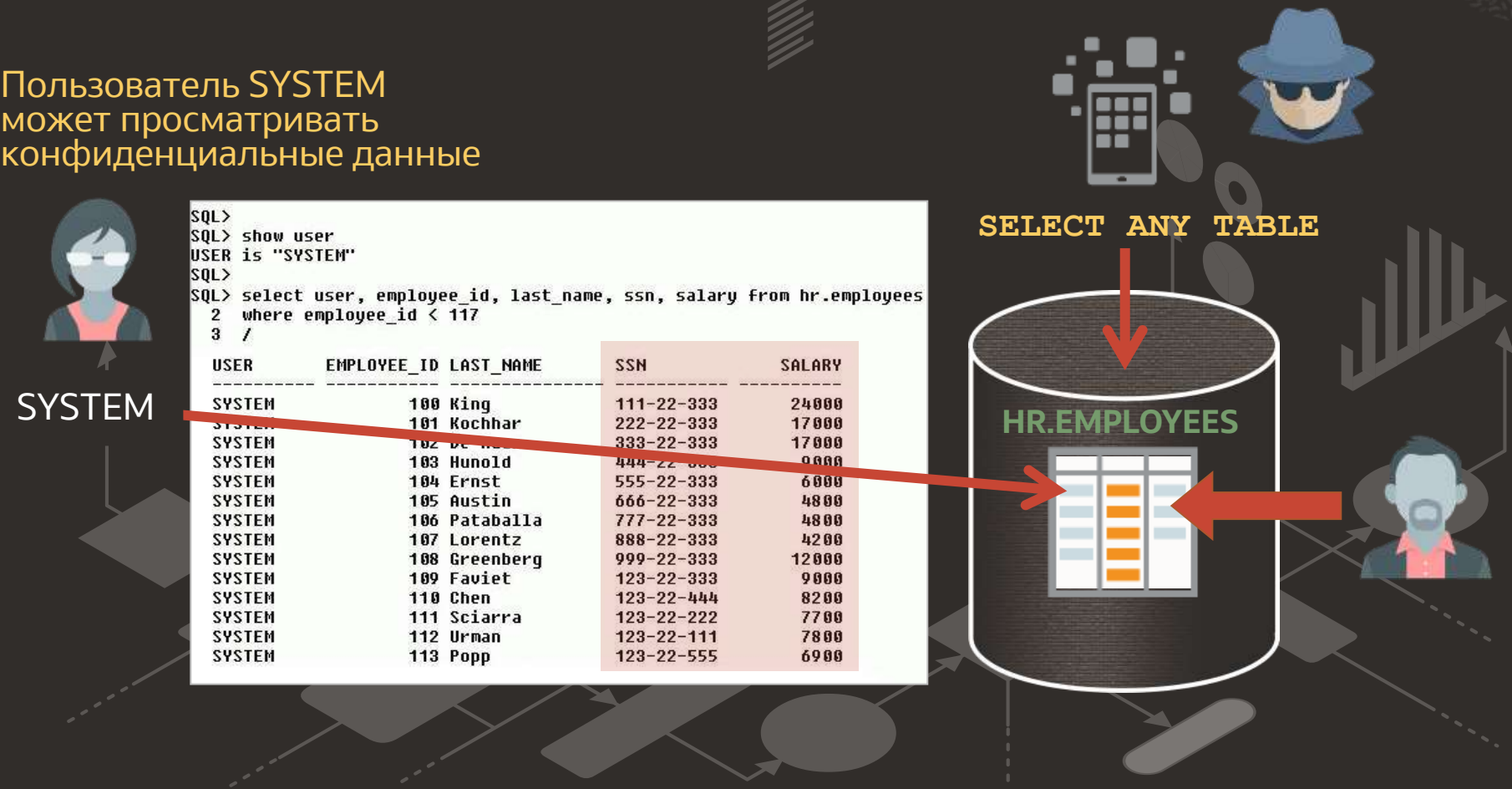
Oracle Database Vault (DBV)

Oracle Database Vault



Oracle Database Vault

Пользователь SYSTEM
может просматривать
конфиденциальные данные

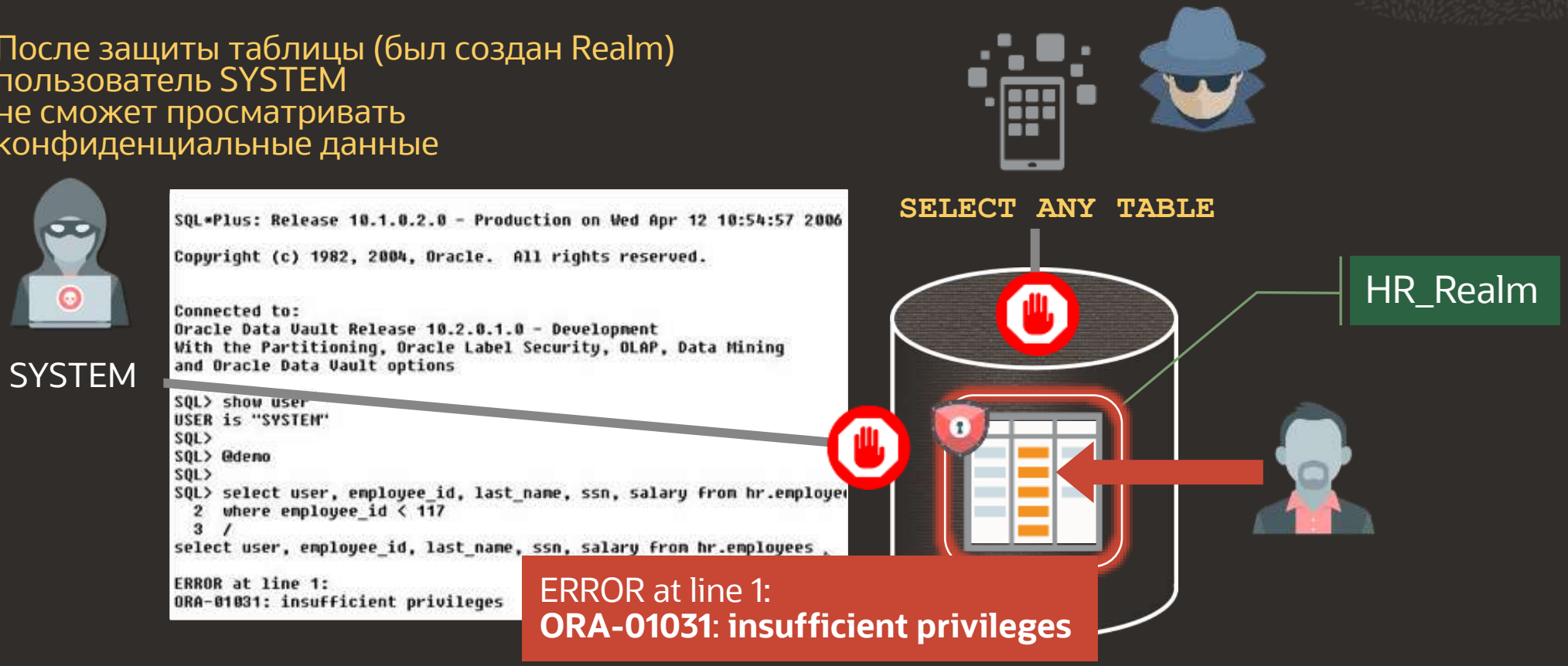



```
SQL>
SQL> show user
USER is "SYSTEM"
SQL>
SQL> select user, employee_id, last_name, ssn, salary from hr.employees
  2  where employee_id < 117
  3  /

USER       EMPLOYEE_ID LAST_NAME       SSN           SALARY
---------- ----------- --------------- ----------- ----------
SYSTEM             100 King            111-22-333       24000
SYSTEM             101 Kochhar         222-22-333       17000
SYSTEM             102 De Haan         333-22-333       17000
SYSTEM             103 Hunold          444-22-333        9000
SYSTEM             104 Ernst           555-22-333        6000
SYSTEM             105 Austin          666-22-333        4800
SYSTEM             106 Pataballa       777-22-333        4800
SYSTEM             107 Lorentz         888-22-333        4200
SYSTEM             108 Greenberg       999-22-333       12000
SYSTEM             109 Faviet          123-22-333        9000
SYSTEM             110 Chen            123-22-444        8200
SYSTEM             111 Sciarra         123-22-222        7700
SYSTEM             112 Urman           123-22-111        7800
SYSTEM             113 Popp            123-22-555        6900
```

Oracle Database Vault

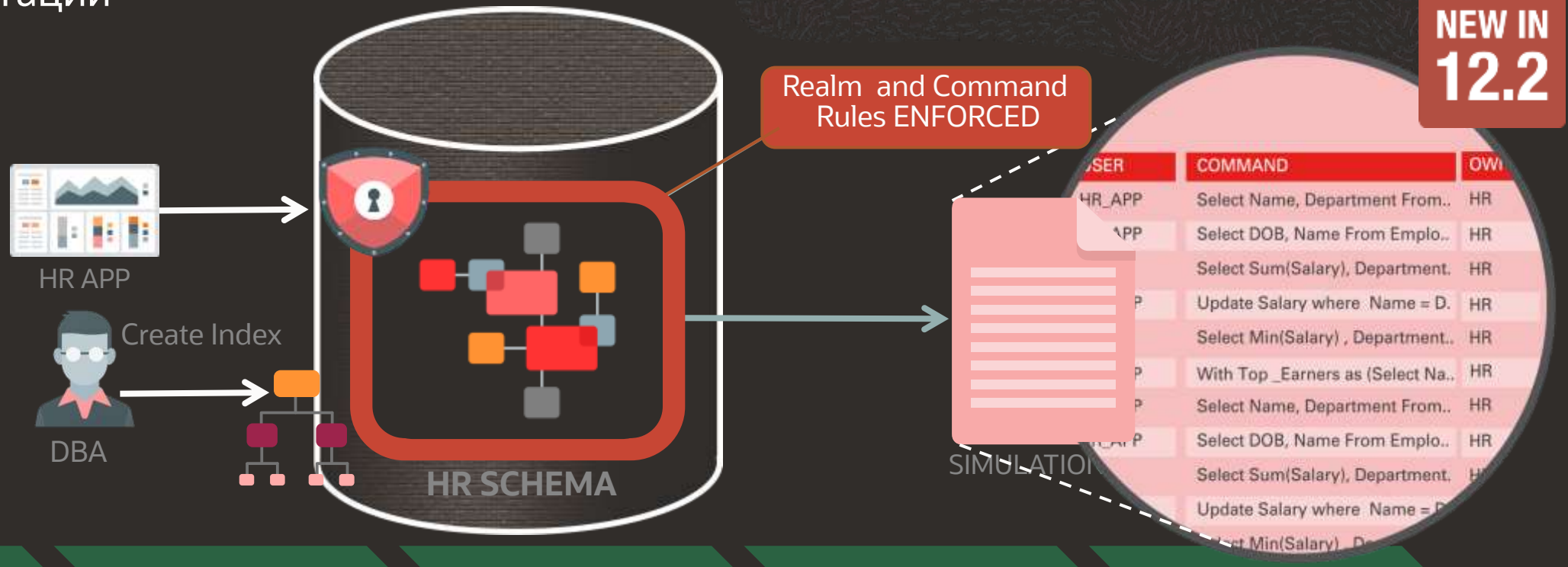
После защиты таблицы (был создан Realm)
пользователь SYSTEM
не сможет просматривать
конфиденциальные данные



*) Факты попыток несанкционированного доступа регистрируется средствами встроенного аудита

Oracle Database Vault

Режим имитации



NEW IN 12.2

Development	Integrated Test	Production Test	Production	Activate New Profile
Create DV profile Protected Objects	Regression testing Authorized Users	Devops/Patching Authorized Tasks	Trusted path factors IPs, Users, Modules	

DBSAT

AVDF

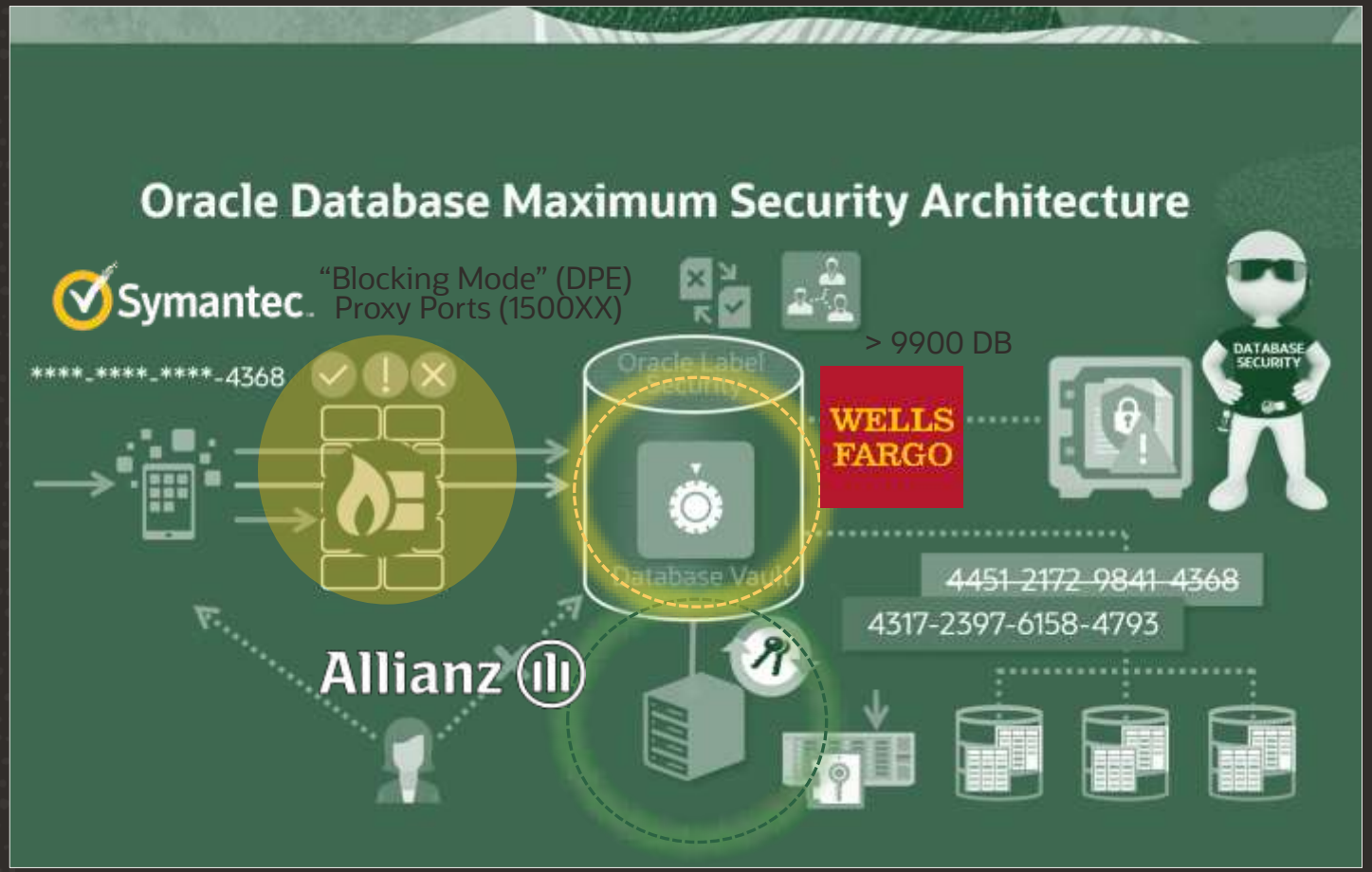
ASO

Key Vault

Masking Pack

Label Security

DBV



Николай Данюков

Ведущий консультант, Oracle в России и СНГ

ORACLE