IBM Security
Intelligence. Integration. Expertise.

IBM

Безопасность данных. Как защитить данные и пройти аудит?

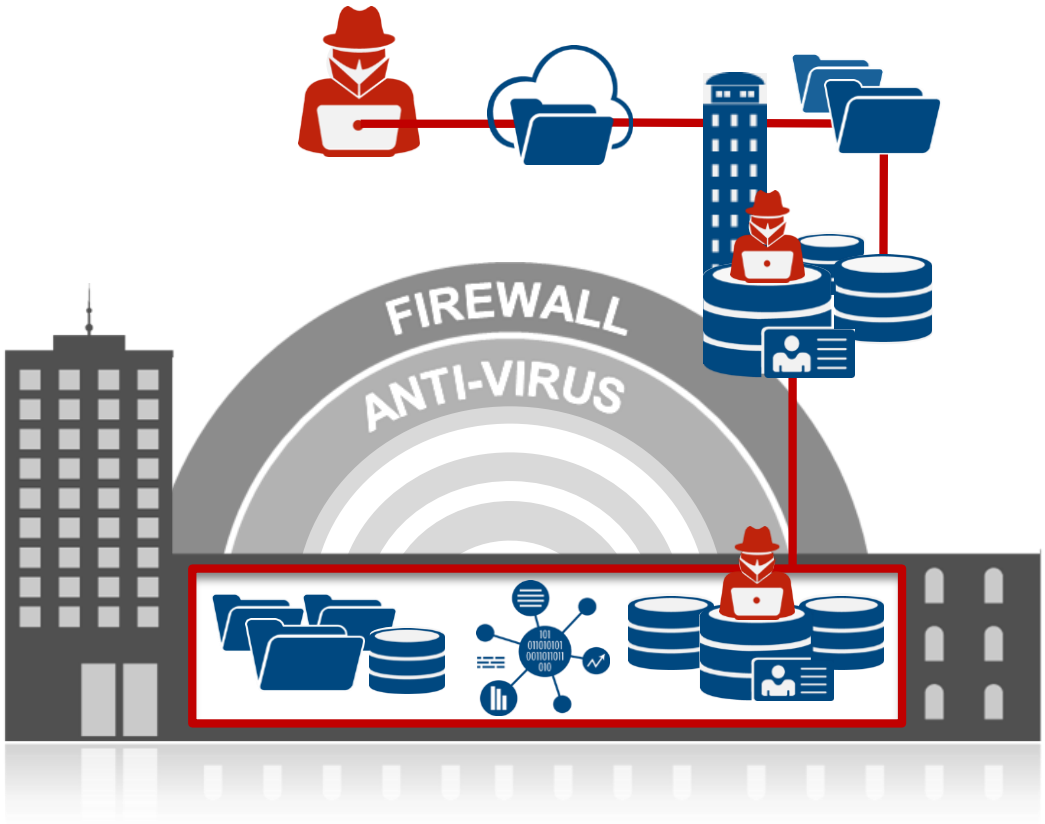
IBM Security Guardium Data Protection

Денис Кириченко

IBM Guardium

- Зачем нужен Guardium ?
- Обзор решения
- Интеграция с продуктами IBM Security
- Уникальные особенности
- Результаты внедрения

Достаточно ли традиционных контролей?



70% Ценности организации

1. Внутренние угрозы
2. Внешние угрозы
3. Регуляторы

Зачем нужен Guardium ?

Угрозы

- Неавторизованные изменения
- Предотвращение утечек данных

Нормативные требования

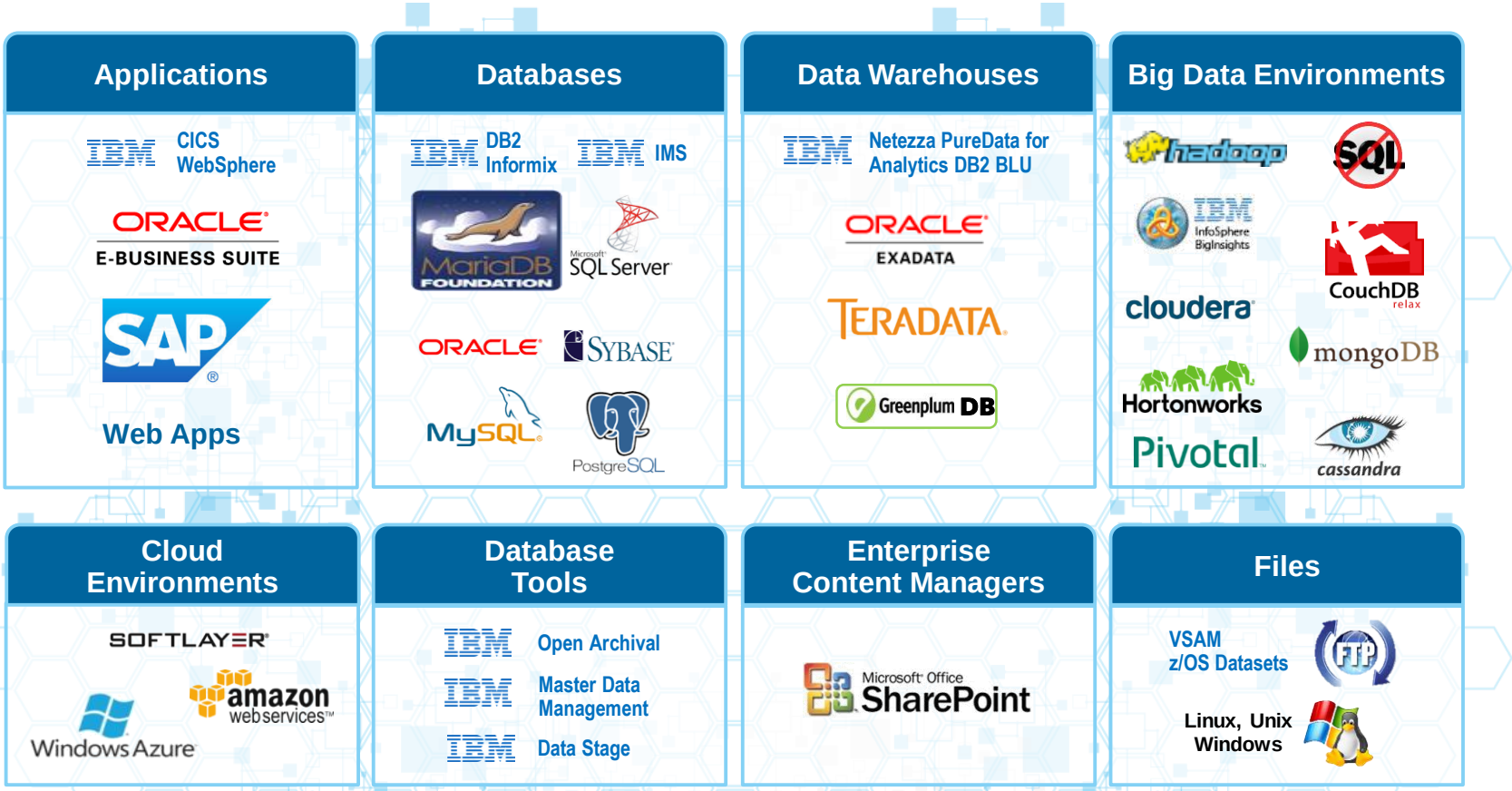
- Упрощение и автоматизация процессов
- Сокращение времени аудита

Уменьшение нагрузки на СУБД

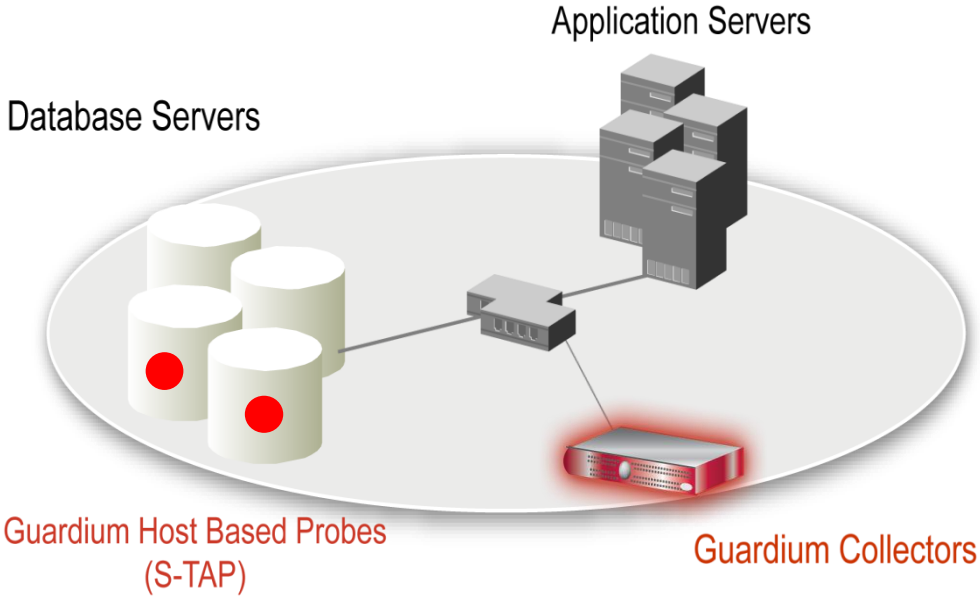
- Замена нативного аудита
- Сокращение затрат!!!

Решение IBM Security Guardium

Поддержка разных систем



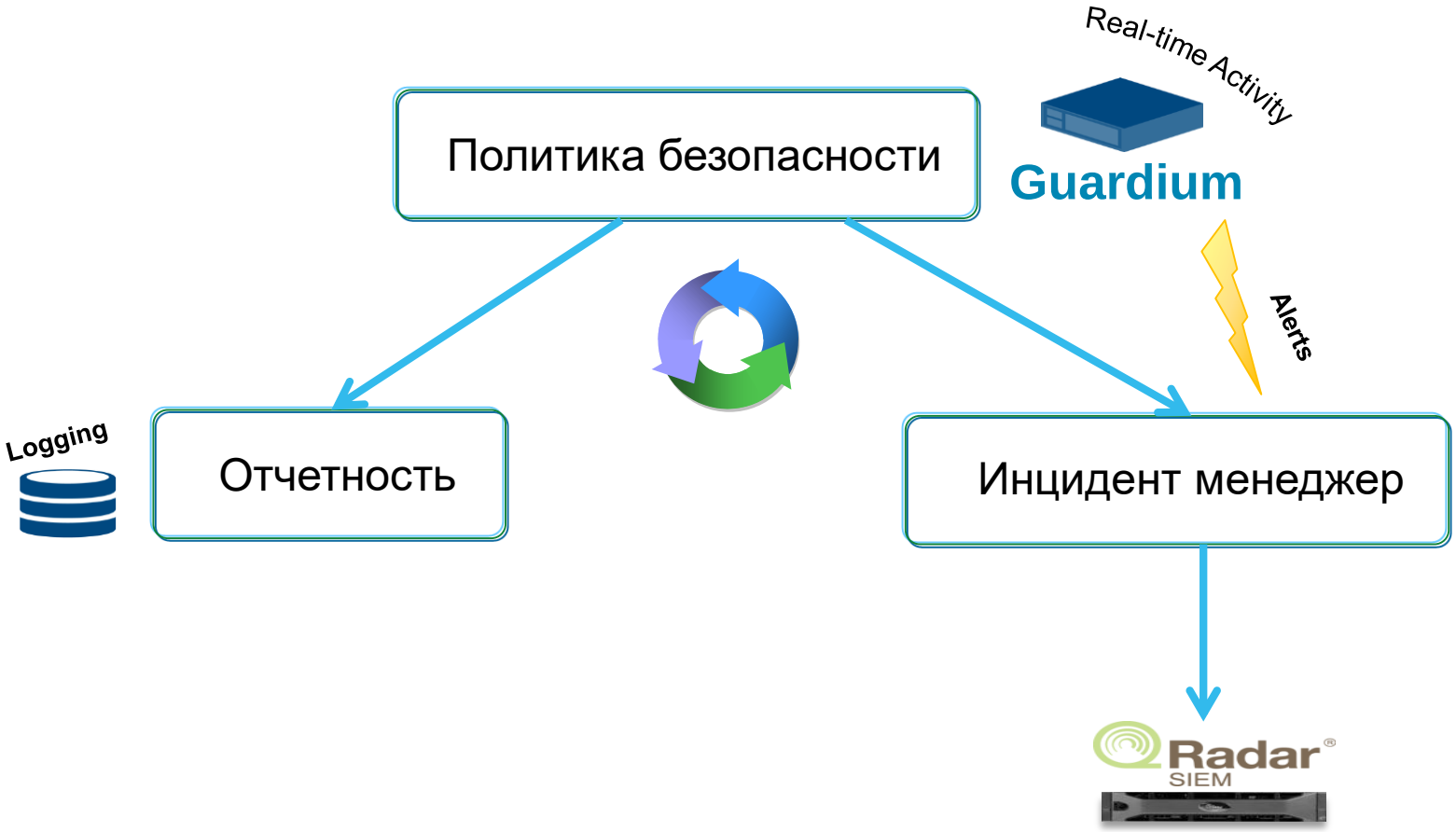
Мониторинг БД в реальном времени



- Продуманная архитектура
- Универсальное решение для разных СУБД
- 100% контроля, включая локальный доступ DBA

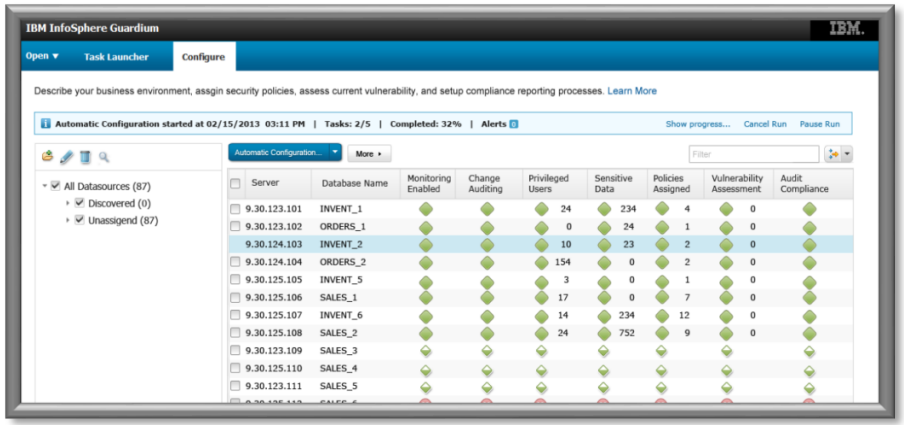
- Не полагается на логи в БД, которые могут быть стерты
- Детальные политики и аудит
- Автоматическая отчетность (SOX, PCI, NIST, и т.д.)

Guardium с точки зрения пользователя

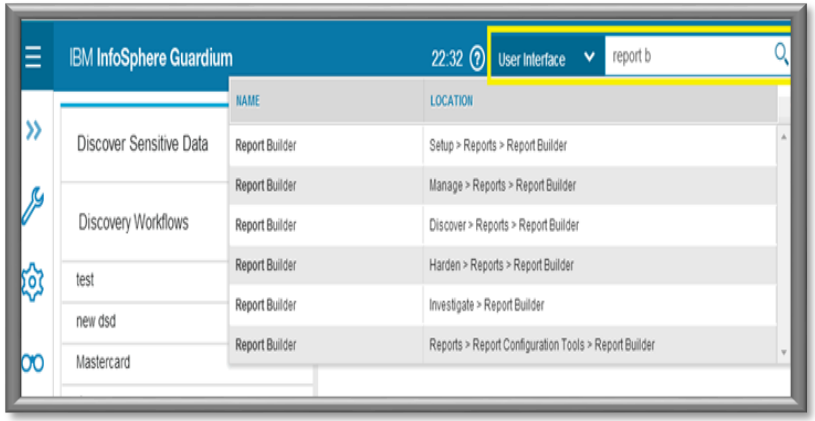


Политика безопасности (правила мониторинга)

- Состоит из правил
- Можно использовать несколько политик
- Набор встроенных политик (PCI и т.д.)
- Может быть сформирована автоматически
- Правило – критерии срабатывания и реакции
- Правила трёх типов:
  - доступ (запросы)
  - извлечение (ответы)
  - исключение (ошибки)



Оценка уязвимости БД (Vulnerability Assessment)



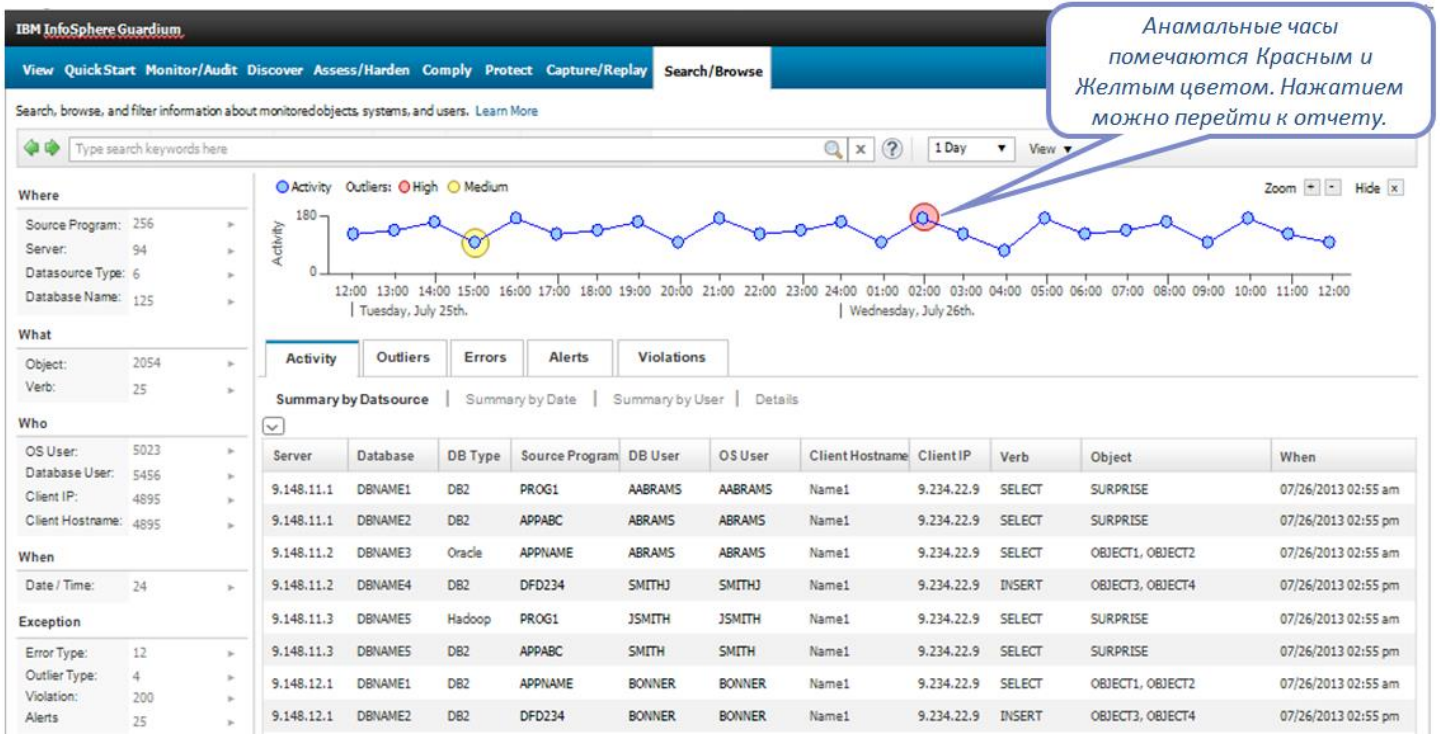
- Дополнительный модуль
- Анализ базового состояния
- Настраиваемые тесты
  - Скрипты ОС, SQL-запросы к СУБД, файлы...
- Проверки:
  - Конфигурация СУБД
  - Файлы ОС
  - Активность в СУБД

Guardium интеграция с продуктами линейки Security

- Guardium сообщает об инцидентах в Qradar
  QRadar дополняет информацией из других источников
  Преимущества: Полная картина инцидента

- Guardium сканирует уязвимости БД и передает в QRadar
  Преимущества: Все уязвимости в единой консоли

Уникальные особенности – Аномальная активность



Server	Database	DB Type	Source Program	DB User	OS User	Client Hostname	Client IP	Verb	Object	When
9.148.11.1	DBNAME1	DB2	PROG1	AABRAMS	AABRAMS	Name1	9.234.22.9	SELECT	SURPRISE	07/26/2013 02:55 am
9.148.11.1	DBNAME2	DB2	APPABC	ABRAMS	ABRAMS	Name1	9.234.22.9	SELECT	SURPRISE	07/26/2013 02:55 pm
9.148.11.2	DBNAME3	Oracle	APPNAME	ABRAMS	ABRAMS	Name1	9.234.22.9	SELECT	OBJECT1, OBJECT2	07/26/2013 02:55 am
9.148.11.2	DBNAME4	DB2	DFD234	SMITHJ	SMITHJ	Name1	9.234.22.9	INSERT	OBJECT3, OBJECT4	07/26/2013 02:55 pm
9.148.11.3	DBNAME5	Hadoop	PROG1	JSMITH	JSMITH	Name1	9.234.22.9	SELECT	SURPRISE	07/26/2013 02:55 am
9.148.11.3	DBNAME5	DB2	APPABC	SMITH	SMITH	Name1	9.234.22.9	SELECT	SURPRISE	07/26/2013 02:55 pm
9.148.12.1	DBNAME1	DB2	APPNAME	BONNER	BONNER	Name1	9.234.22.9	SELECT	OBJECT1, OBJECT2	07/26/2013 02:55 am
9.148.12.1	DBNAME2	DB2	DFD234	BONNER	BONNER	Name1	9.234.22.9	INSERT	OBJECT3, OBJECT4	07/26/2013 02:55 pm

- Поиск аномального поведения в большом количестве данных
- Адаптивный динамический алгоритм для моделирования шаблона поведения поступающих данных (Machine Learning)

Уникальные особенности – Динамическое маскирование

- Маскирование значений чувствительных данных – замена значе***

  Горизонтально – по строкам
  Вертикально – по колонкам

- Возможность использовать продуктивные данные для тестирования

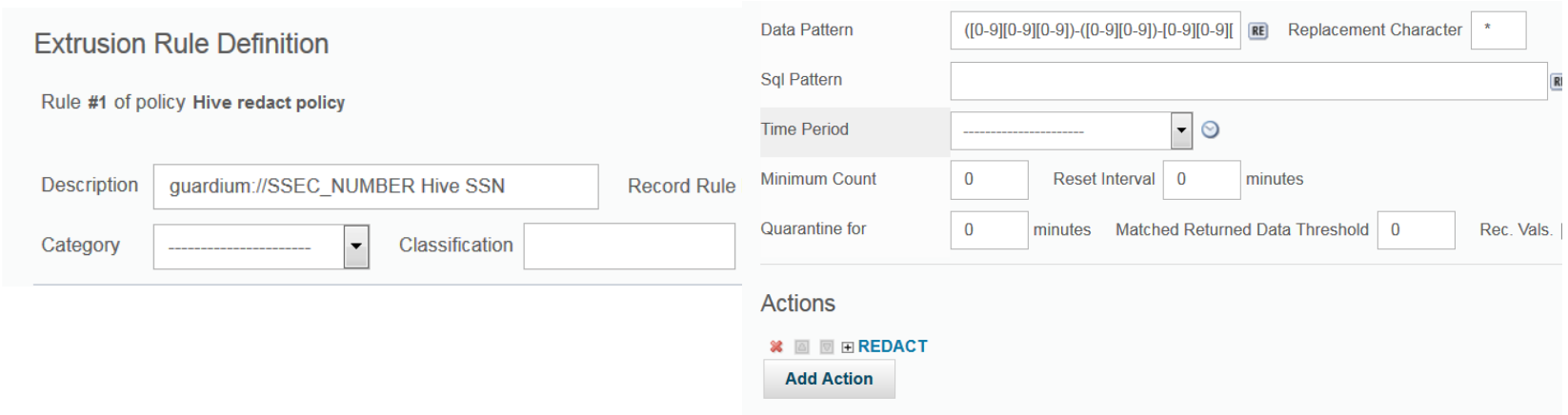
- Ограничение просмотра для операторов данных

```
SQL> select email from customer_demo1;

EMAIL2
----------------------------------------
Joe.Ant****
Joe.Tho****
Joe.Smi****
Joe.Jon****
Joe.Mur****
Joe.Sha****
Joe.Kin****
Joe.Lyn****
Joe.Lee****
Joe.Dav****
Joe.Wil****

11 rows selected.
```

Маскирование разных данных (Hive, BigSQL, SQL)



Маскированные данные Hive в Hue/Beeswax

	credit_card_details.name	credit_card_details.cc_format1	credit_card_details.cc_phone	credit_card_details.cc_ssn
0	'John Doe'	'**********0001'	'370-008-1224'	'***-**-8412'
1	'Jane Doe'	'**********0002'	'370-800-6880'	'***-**-8412'
2	'John Smith'	'**********0004'	'333-666-4444'	'***-**-8412'

Маскированные данные Hive в коммандной строке

```
0: jdbc:hive2://cloudera-cl1-01.guard.swg.usm> select * from credit_card_details;
+---------------------------+-----------------------------------+-------------------------------+-----------------------------+--+
| credit_card_details.name  | credit_card_details.cc_format1    | credit_card_details.cc_phone  | credit_card_details.cc_ssn  |
+---------------------------+-----------------------------------+-------------------------------+-----------------------------+--+
| 'John Doe'                | '**********0001'                  | '370-008-1224'                | '***-**-8412'               |
| 'Jane Doe'                | '**********0002'                  | '370-800-6880'                | '***-**-8412'               |
| 'John Smith'              | '**********0004'                  | '333-666-4444'                | '***-**-8412'               |
+---------------------------+-----------------------------------+-------------------------------+-----------------------------+--+
```

Выбор мировых лидеров рынка

- 8 из Топ-10 Банков
- 5 из Топ-6 Страховых компаний
- 4 из Топ-4 Медицинских организаций
- 8 из Топ-10 Телекомов
- 3 из Топ-4 Авто производителей
- 3 из Топ-3 Производителей напитков
- 2 из Топ-3 Сетей магазинов

Выбор мировых лидеров рынка

Выбор лидеров рынка России и СНГ

Внедрения в РФ - Телеком

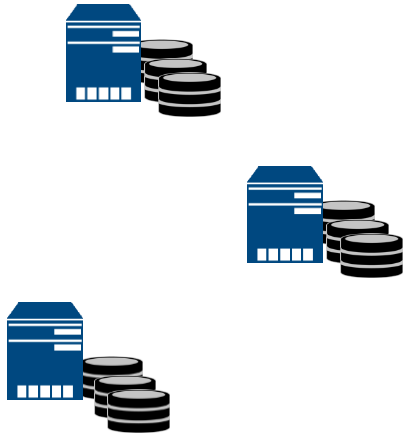
- **Кто:** 4 крупнейших операторов сотовой связи РФ
- **Задача:** защита персональных данных абонентов в соответствии с ФЗ-152
- **Среды:** распределённые ЦОД (основной - резервный)
  - СУБД: Oracle, MS SQL Server
  - ОС: Solaris
  - Приложения: биллинг и CRM-система
- **Результат:**
  - Мониторинг доступа к объектам БД с ПДн в приведённых системах
  - Мониторинг событий безопасности (ошибок, неудачных входов)
  - Контроль действий администраторов и разработчиков
  - Интеграция с системами мониторинга ИБ (SIEM)
  - Оповещения об инцидентах ИБ
  - Возможность применения единой политики безопасности на все СУБД

Внедрения в РФ - Банки

- **Кто:** крупный розничный банк, крупный универсальный банк, крупный частный банк
- **Задача:** прохождение аудита PCI-DSS и ФЗ-152
- **Среды:** распределённые ЦОД (основной - резервный, высокая доступность)
  - СУБД: Oracle, Teradata
  - Приложения: процессинговая система, CRM-система
- **Результат:**
  - Успешное прохождение аудита PCI-DSS
  - Мониторинг доступа к объектам БД с ПДн в приведённых системах
- Мониторинг событий безопасности (ошибок, неудачных входов)
- Контроль действий администраторов и разработчиков
- Контроль действий конечных пользователей приложений
- Отсутствие изменений в СУБД

Лицензирование

- Новая упрощенная система лицензирования – один парт номер!
- Необходимо подсчитать количество серверов на которых установлены СУБД, физические и виртуальные
- Используется система Resource Value Units (RVU) основанная на количестве Managed Virtual Servers (MVS)



Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

THANK YOU

www.ibm.com/security

IBM Security

Intelligence. Integration. Expertise.