Актуальные проблемы информационной безопасности в сфере телекоммуникаций и пути их решения

Юрий Филоненко

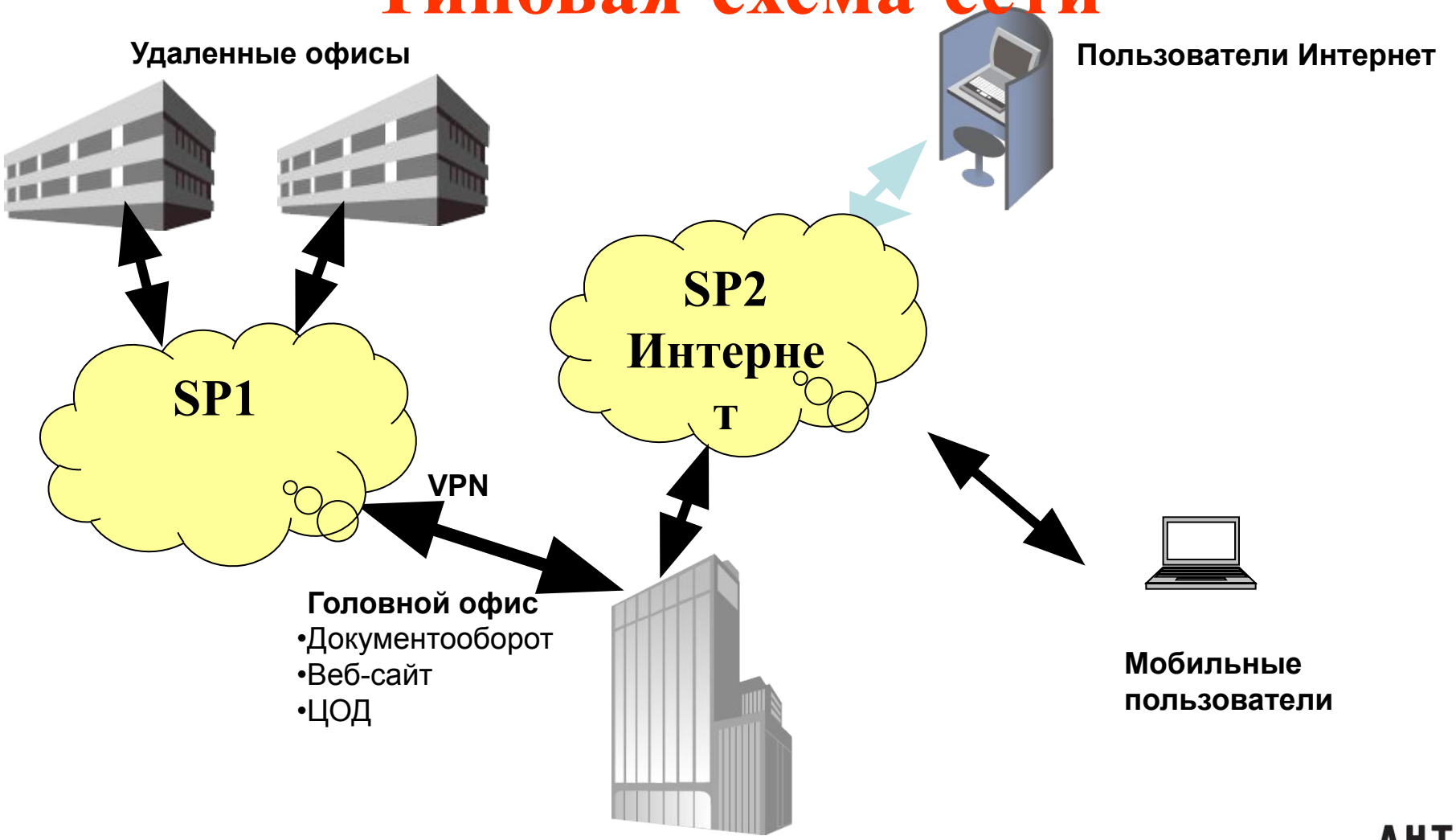
yf@infosafe.ua

- Финансовое мошенничество с помощью кредитных карт
- Угрозы инфраструктуры
- Кража персональных данных
- Кража оборудования
- Угрозы, содержащиеся в веб и mail контенте
- Потенциальные риски

Мошенничество с платежными картами

- Россия – 3-х кратный рост за 2008 год (потери – 1 млрд. рублей)
- Великобритания – рост 20% (потери – 610 млн. фунтов)
  www.apacs.org.uk
- США – рост 33%, потери 265 млн. долларов от онлайновых операций
  www.ic3.gov
- Мир – потери более 1 млрд. долларов

Типовая схема сети



Борьба с угрозами инфраструктуры

- Межсетевые экраны
- IDS/IPS
- VPN-шлюзы
- NAC-шлюзы
- Защита конечных точек
- Шлюзы приложений
- Системы управления
- Управление событиями
- Штатные средства АСО

Кража персональных данных

- 2007 год, сеть магазинов TJX – 46 миллионов номеров платежных карт
- 2008 год, Royal Bank of Scotland – данные 1,5 млн. человек
- 2008 год, Германия – продажа дисков с данными 21 млн. человек (call-центры)
- 2009 год, Heartland Payment Systems – 100 млн. транзакций ежемесячно
- 2009 год, Oklahoma Dpt. Of Human Services – кража ноутбука, 1 млн. записей

Текущая ситуация с персональными данными

- Программами кражи ПД инфицировано 10 млн. компьютеров по всему миру
  http://pandasecurity.com
- 15% респондентов обзора «Персональные данные в России 2008» обрабатывают более 1 млн. записей
  www.perimetrix.ru
- Самая первая кража -1903 год, кража амбулаторных карт в США

Защита персональных данных

- Защита и мониторинг доступа к базам данных
- Противодействие утечкам на уровне конечных точек (DLP)
- Противодействие утечкам на уровне шлюза

Guardium®
SAFEGUARDING DATABASES™

CISCO

McAfee®

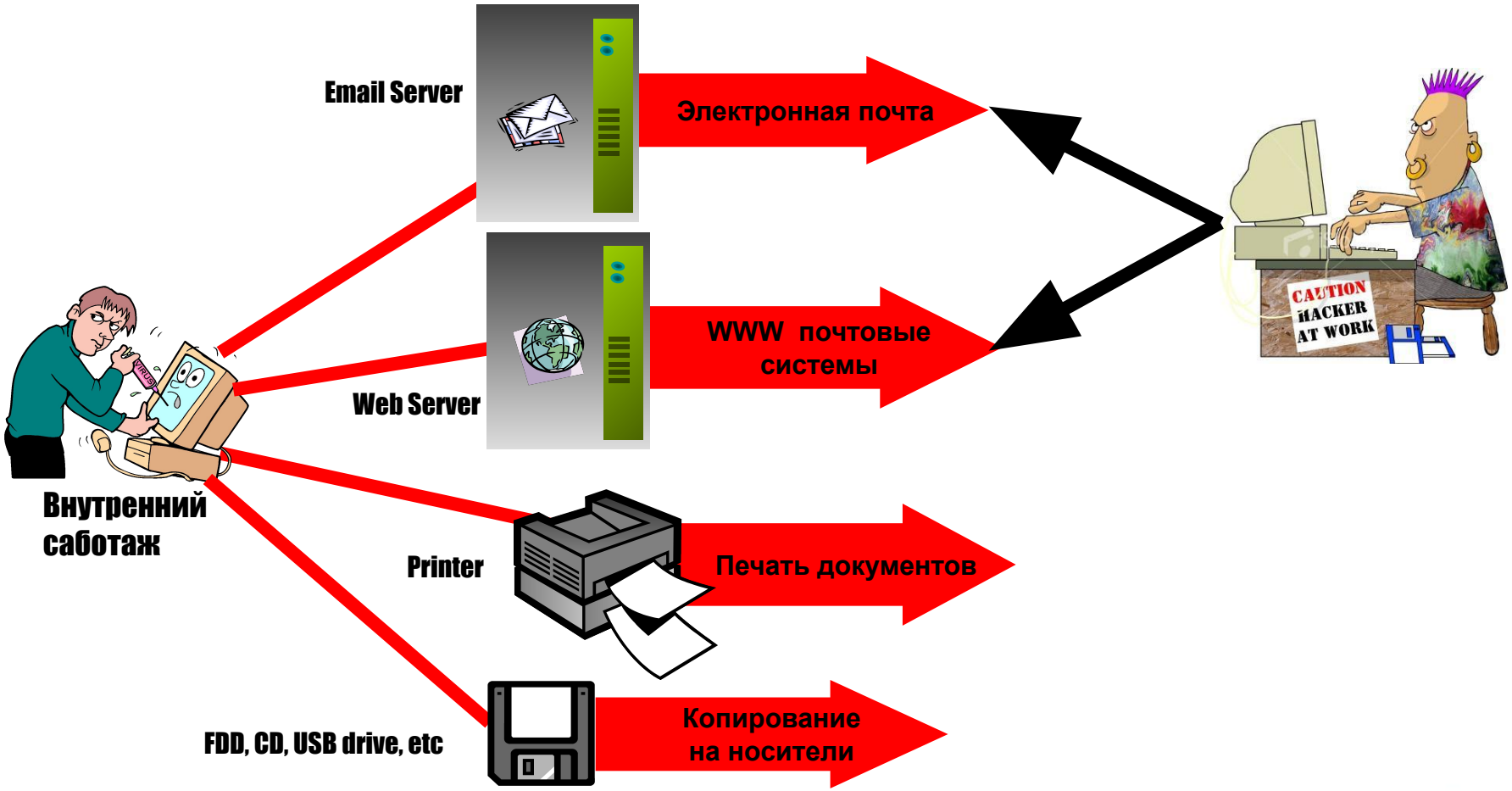
Кража оборудования

- Еженедельно в американских аэропортах теряется более 10000 ноутбуков
  www.pcworld.com
- Защита – аутентификация, криптование, контроль портов
  - Nonstop Laptop Guardium
  - Kaspersky Mobile Security

Alcatel·Lucent

лаборатория КАСПЕРСКОГО

Угрозы в почтовом и веб-контенте



Защита контента

- Система мониторинга и управления ИТ-безопасностью

- Средства защиты контента
  - Anti-spam
  - Anti-malware
  - Anti-virus
  - URL-фильтрация

Система управления IP-guard

Преимущества

IP-guard

- Защита информации
- Разграничение доступа
- Планирование ресурсов
- Контроль данных

Различные модули для различных целей защиты

- Управление доступом к файлам
- Управление печатью
- Управление устройствами
- Контроль сети
- Управление ПО
- Управление веб-доступом
- Управление почтой
- Управление Instant Message
- Снимки экранов
- Управление полосой пропускания
- Управление активами
- Удаленное управление
- Управление съемными носителями
- Базовая информация

Современное состояние безопасности БД

- **В 2009 году усилия по защите информации смещаются от защиты периметра в сторону защиты конфиденциальных данных**
- **Возрастает доля внутренних угроз**
- **Защита информации не должна ухудшать характеристики функционирования бизнес-процессов**
- **Есть необходимость обеспечения соответствия требованиям стандартов в сфере защиты информации**
- **Как основное хранилище важных данных, базы данных становятся основым объектом внимания Служб защиты информации**

Современные вызовы безопасности СУБД

Инфраструктура БД

- Гетерогенная
- Постоянно изменяющаяся

Различные типы доступа к БД

- Сетевые приложения
- Внешний доступ к БД
- Локальный доступ администраторов

Повышенная производительность

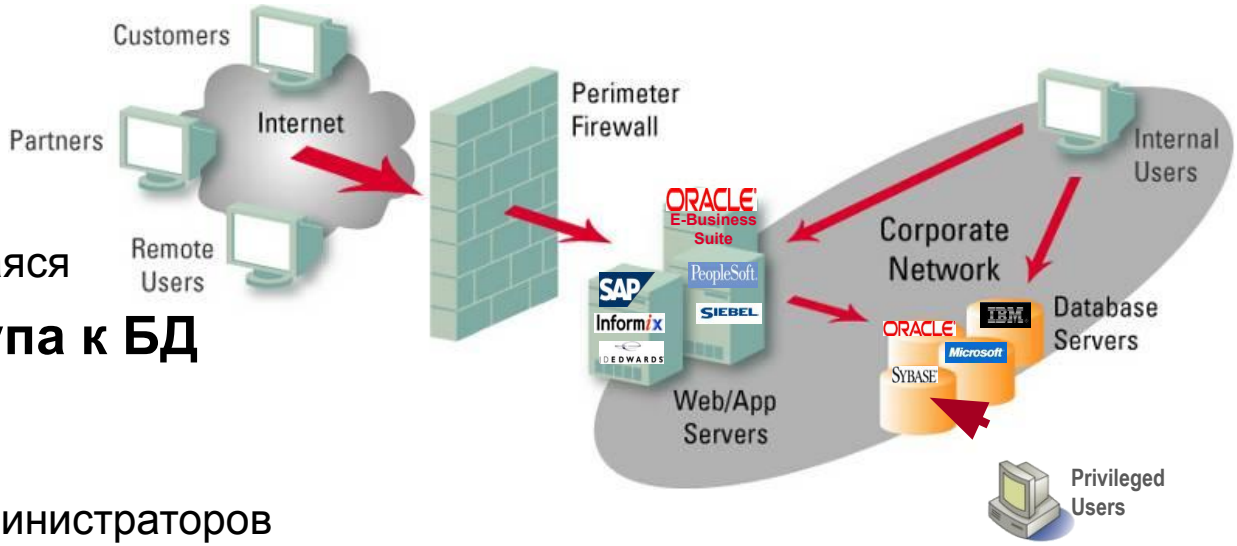
- Критичные для бизнеса приложения
- Подверженность манипуляциям

Распределение полномочий

- СУБД/Инфрастуктура
- Безопасность/Аудит

Широкое использование журналов СУБД

- Первая логичная мера мониторинга доступа к БД



Недостатки традиционного журналирования

1. Проблемы детализации

- Трудности мониторинга привилегированных пользователей
- Трудности мониторинга пользователей приложений

2. Влияние на производительность

- Слабая ориентированность на безопасность
- Значительная нагрузка на ЦП

3. Различные методы для разных СУБД

- Отсутствие унифицированного подхода к безопасности
- Неэффективно и небезопасно

4. Проблема хранения, отчетности и прогнозирования

- Требования к размеру хранилища данных аудита
- Сложность аудита и прогнозирования

5. Проблема защиты в реальном времени

- Вопрос уведомления об аномалиях
- Нет возможности блокирования вредоносных действий

6. Нет разграничения полномочий

1. DBA не выполняет функции защиты
- DBA не могут мониторить сами себя

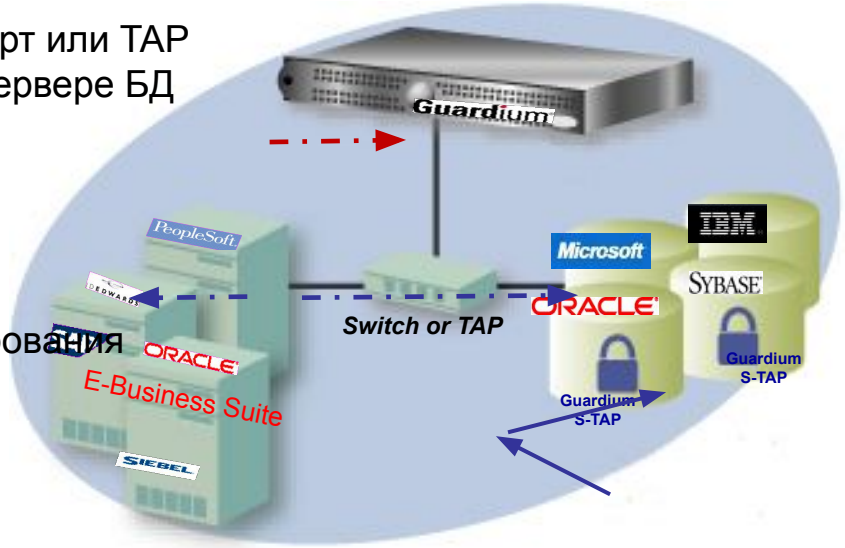
Система мониторинга БД **Guardium**

Исчерпывающий мониторинг и контроль изменений

- Мониторинг всего SQL траффика через SPAN порт или TAP
- Мониторинг лок. доступа с помощью агента на сервере БД
- Возможность уведомлений и блокирования НСД
- Контроль изменений файлов и конфигураций

Независимость от СУБД

- Не зависит от встроенных механизмов журналирования
- Не влияет на производительность СУБД
- Не требует изменения СУБД и ПО
- Защита от DBA



Агенты, установленные для мониторинга локального доступа DBA

Единое решение для гетерогенной среды

- Поддержка Oracle, MS SQL, IBM DB2, MySQL, и т.д.
- Поддержка SAP, Oracle EBS, Siebel, приложений заказчика
- Поддержка Windows, Linux, Solaris, AIX, HP UX, z/OS и т.д.

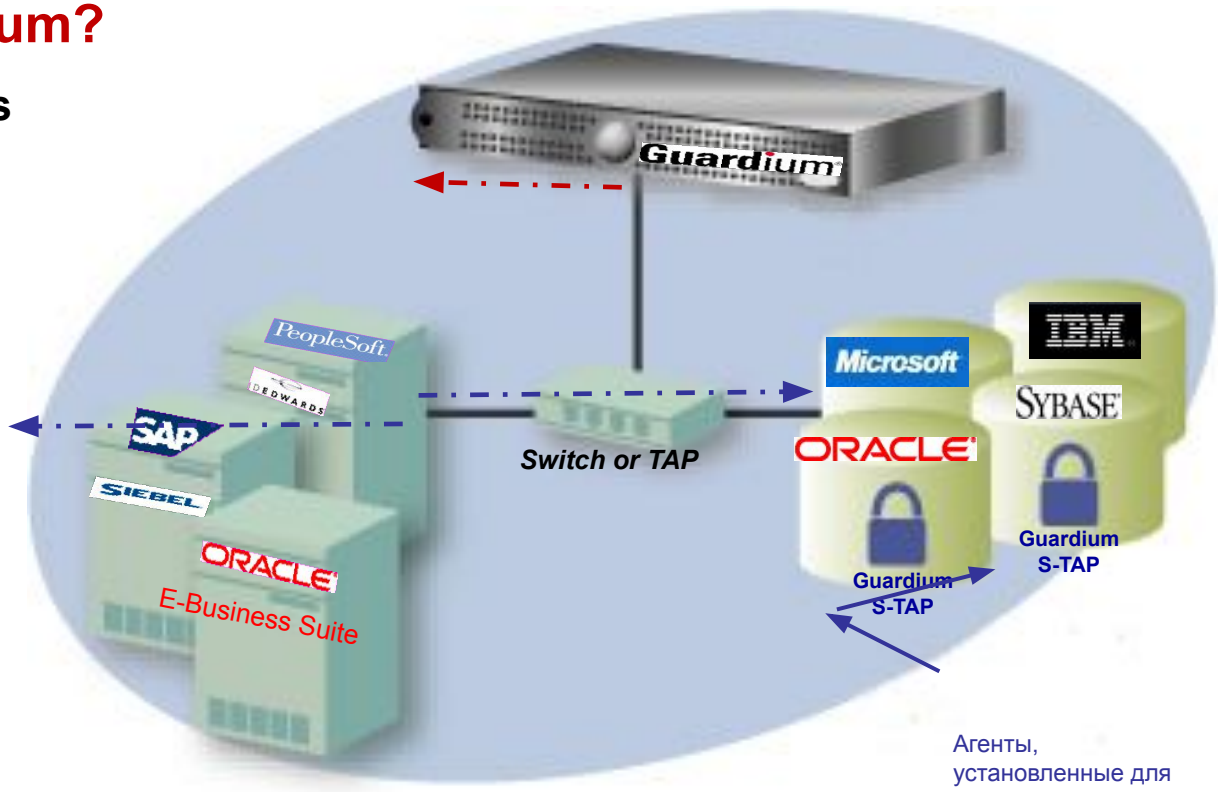
Автоматизированная отчетность

- Стойкое и защищенное хранилище данных для отчетов
- Создание шаблонных либо уникальных отчетов по расписанию
- Управление соответствием

Исчерпывающий мониторинг SQL

Что отслеживает Guardium?

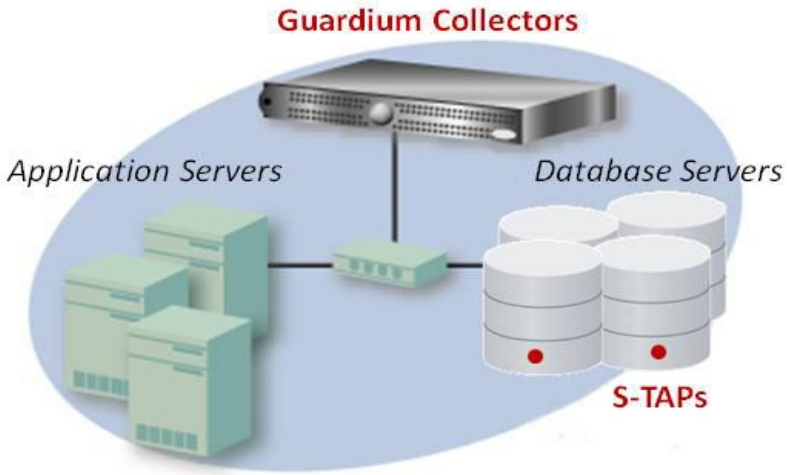
- **SQL Errors and failed logins**
- **DDL commands**
  (Create/Drop/Alter Tables)
- **SELECT queries**
- **DML commands**
  (Insert, Update, Delete)
- **DCL commands**
  (GRANT, REVOKE)
- **Procedural languages**
- **XML executed by database**



Агенты, установленные для мониторинга локального доступа DBA

Агент **S-TAP** обеспечивает полную наблюдаемость

- Дополнительное легковесное решение, устанавливаемое на сервер БД и работающее на уровне IPC ОС
- Перехватывает 100% действий, включая TCP, общую память, Oracle BEQ, named pipes, TLI, и IPC-соединения
- Направляет информацию устройству Guardium для обработки
- Не требует изменения в конфигурации БД
- Обеспечивает перехват 1000 записей аудита в секунду с 3% потерей производительности
- S-GATE для блокирования соединений



Выводы

- ✔ Безопасность – это задача всех служб
- ✔ Безопасность – это непрерывный процесс
- ✔ Безопасность – обеспечивается во всех точках
- ✔ Безопасность – инновационная деятельность
- ✔ Безопасность – это выгодное вложение средств

Контакты

Антивирусная Лаборатория

03037 Киев, проспект Краснозвездный, 54
тел.: +38 (044) 494-15-15 (многоканальный)
Общая информация: info@virusam.net
Отдел продаж: sales@virusam.net
Управление проектами: projects@virusam.net