Imperva

Эффективные решения для защиты приложений баз данных

iMPERVA®

О компании

- Миссия
  - Создание эффективных и универсальных решений для защиты приложений баз данных
- Лидерство в областях
  - Защита Web-приложений
  - Аудит, мониторинг и защита баз данных
- Год образования - 2002 г., Начало производства - 2003 г.
- Место расположения:
  - Штаб квартиры в США (Калифорния) и Израиль
  - Локальные представительства: Великобритания, Франция, Германия, Япония, Китай, Тайвань
- 50 компаний-дистрибуторов
- Более 300 заказчиков
- Президент и генеральный директор - Шломо Крамер (один из основателей компании Check Point)

Проблема кражи данных

- Борьба с кражами данных – актуальная и жизненно важная проблема
  - 85% организаций сталкивались с проблемой
  - За период 2005-2008 гг. было украдено **226,970,321** записей СУБД

- … и обходится дорого:
  - Оценочная стоимость одной записи СУБД
    - **$182**
  - Из всех компаний, которые сталкивались с проблемой:
    - ~75% сообщали об этом своим клиентам
    - ~60% столкнулись с судебными разбирательствами
    - 33% заплатили штраф
    - 32% понесли убытки за счет снижения стоимости акций

Общий убыток: **$28,764,786,232.00**

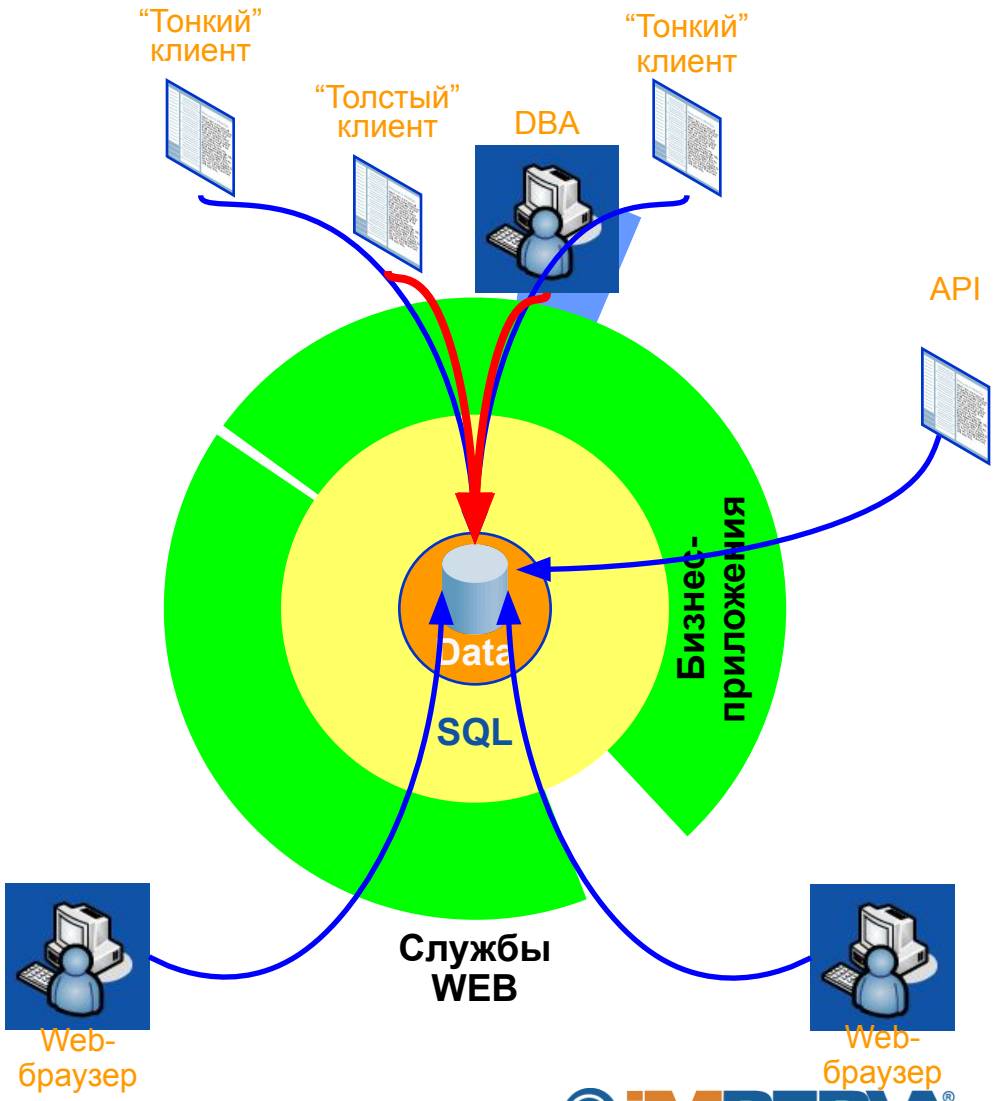
Что украдено (яркие примеры)

- США:
  - База с персональными сведениями о 30 млн. бывших и нынешних военнослужащих США (2006 г).
  - База клиентов сети розничных магазинов TJX Cos (США) с 45,7 млн номерами банковских карт (2007 г.)

- Россия:
  - База данных абонентов МТС (2003 г.)
  - База данных о банковских проводках расчетно-кассовых центров ЦБ РФ за 2003-2004 гг. (2005 г.)
  - База данных абонентов “Корбина телеком” (2007 г.)
  - ?

Механизмы доступа к данным

- Непосредственный доступ
  - Для администраторов через механизм SQL запросов
  - Для локальных пользователей с помощью технологии “толстых” клиентов (Visual Basic)
- Доступ для локальных пользователей посредством “тонких” клиентов” бизнес-приложений (SAP, E-Business Suite, Peoplesoft и др.)
- Доступ локальных и внешних пользователей посредством Web - браузеров и Web API



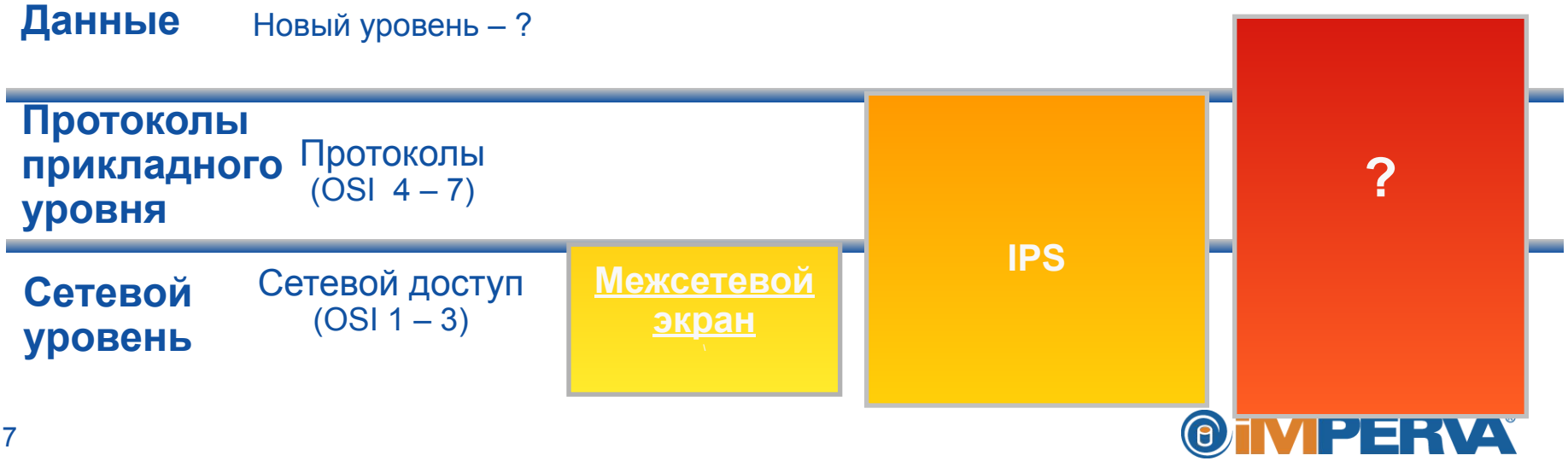
Требования стандарта PCI

- В соответствии со требованиями стандарта PCI :
  - Необходимо наличие межсетевого экрана с функциями защиты на прикладном уровне (**Application layer firewall)** либо проведение аудита исходного кода приложения (требование # 6.6)
  - мониторинг доступа к персональным данным держателей кредитных карт (требование #10)

- Продукты линейки SecureSphere полностью удовлетворяют требованиям # 6.6 и #10 стандарта PCI
- Компания Imperva является действующим членом Совета *PCI Security Standards Council*

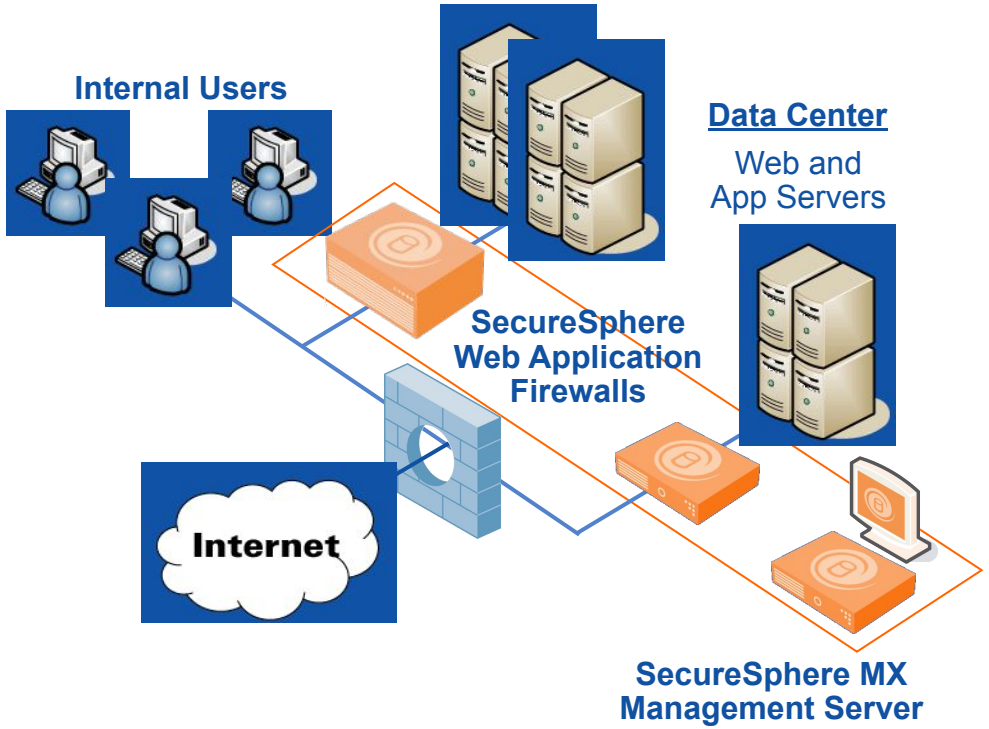
Необходимость обеспечения защиты данных

- Межсетевые экраны эффективны против атак на сетевом уровне
- IPS эффективны для борьбы с атаками на протоколы прикладного уровня
- Для борьбы с атаками на сами данные необходимы иные средства



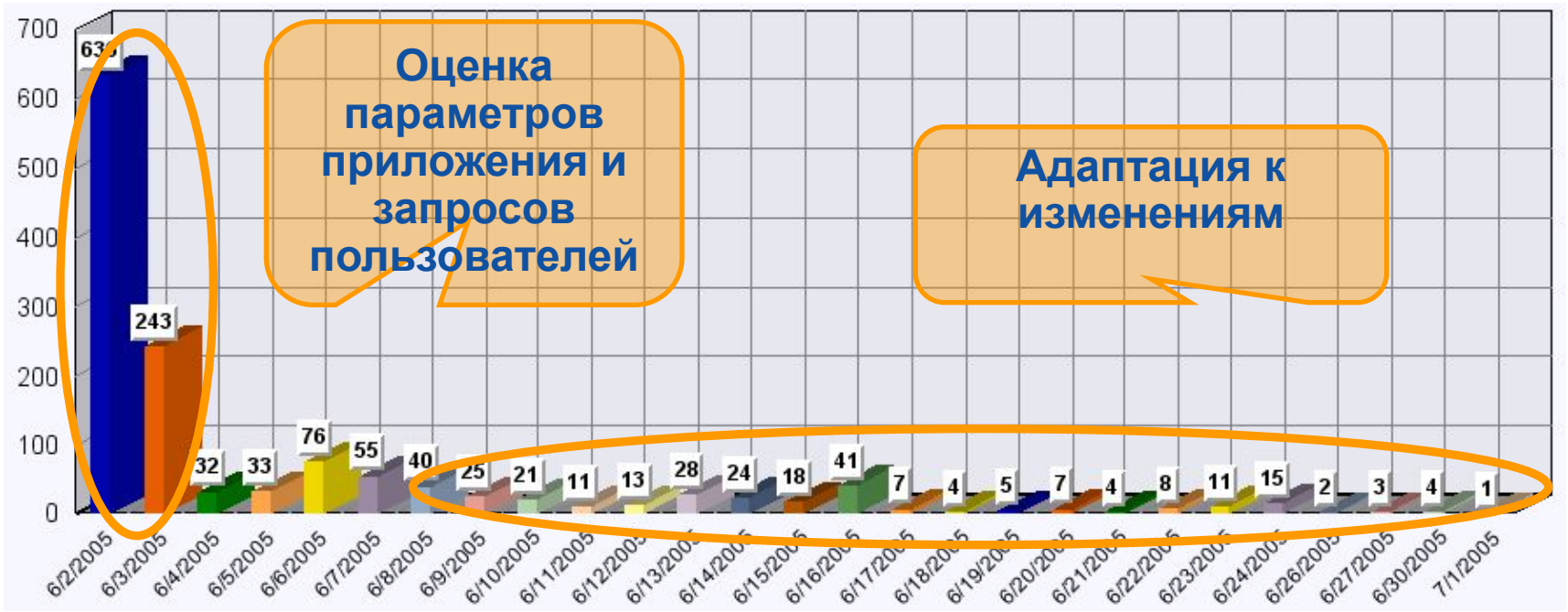
Что такое Imperva SecureSphere

- Комплексное решение для защиты приложений баз данных
- Мониторинг, аудит и безопасность баз данных
- Более 350 инсталляций



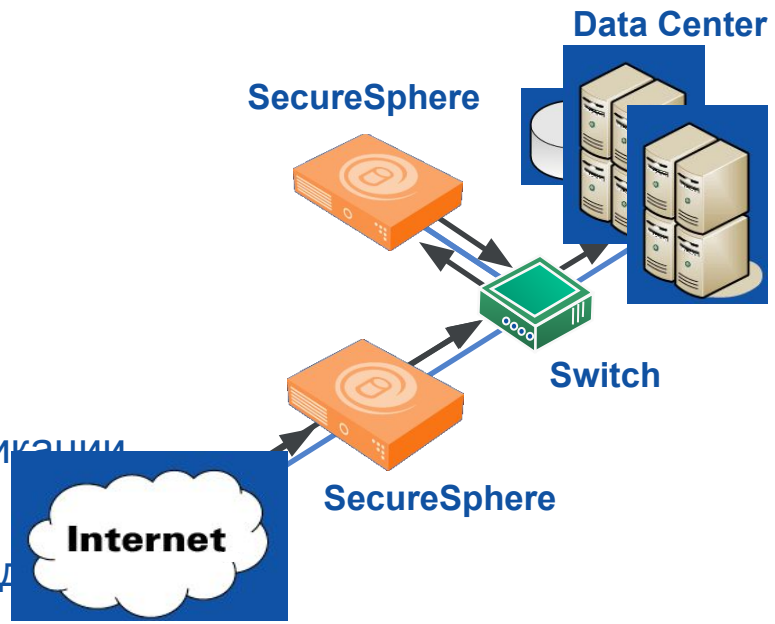
Динамическое профилирование

- Автоматическая настройка правил (политик)
- Автоматическое обучение по параметрам (структура приложения, элементы, характер запросов пользователей)
- Снижение административных затрат (5-15 изменений профиля в неделю ~ 5-30 чел./ч)



Варианты развертывания

- Transparent Inline Bridge
  - Поддержка всех функций
  - Высокая производительность, низкие задержки
  - Отказоустойчивый режим работы интерфейсов (Fail-open/ByPass)
- Transparent & Reverse Proxy
  - Высокая производительность модификации контента
  - Перезапись URL, цифровые подписи д cookie,
    терминирование SSL-сессий
- Non-inline
  - Мониторинг, отсутствие влияние на прохождение пакетов



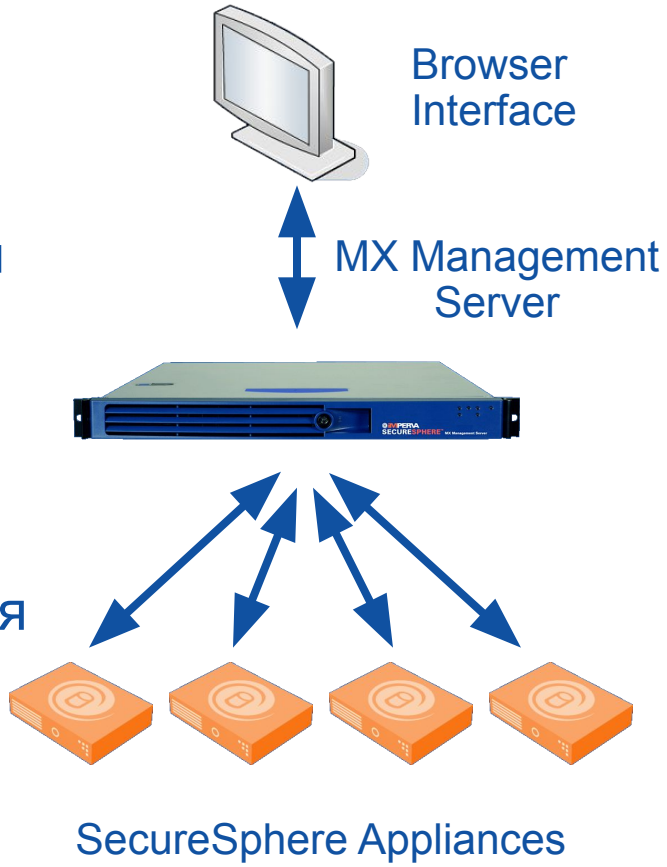
- Sniffer Mode

Типовой сценарий развертывания

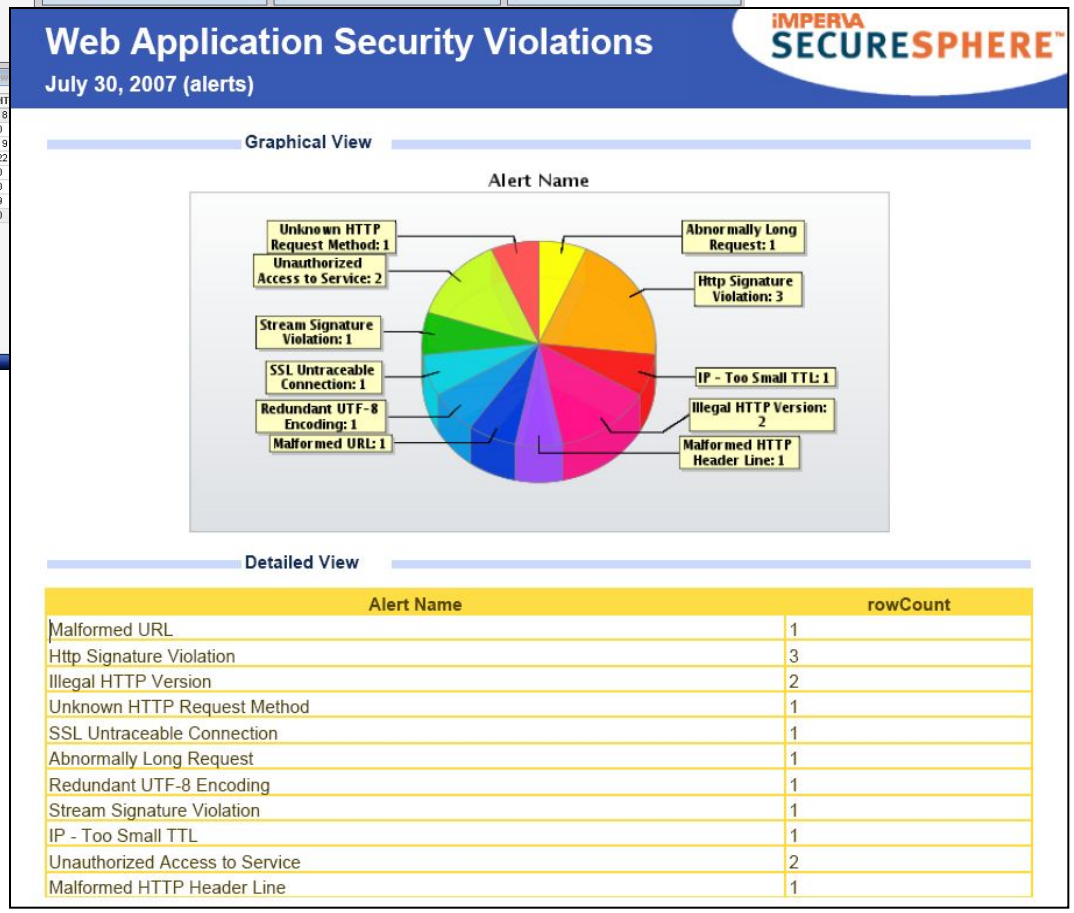
- Установка в течение нескольких минут
  - Отсутствие необходимости внесения изменений в приложения и сетевую структуру
- Мгновенная защита от известных угроз
- Защита от принципиально новых угроз после окончания процесса динамического профилирования (2-5 дней)
- Высокая доступность:
  - Интерфейсы с режимом Fail-open (самый экономичный способ)
  - A/P или A/A кластеры (IMPVHA, VRRP)

Принципы управления

- Централизация
  - Управление всеми устройствами из единой web-консоли
  - Интегрированные механизмы аудита и генерации отчетов
  - Простота развертывания новых устройств
  - Иерархическая структура управления политиками
- Контроль доступа на основе ролей



Графические отчеты



Alert Name	rowCount
Malformed URL	1
Http Signature Violation	3
Illegal HTTP Version	2
Unknown HTTP Request Method	1
SSL Untraceable Connection	1
Abnormally Long Request	1
Redundant UTF-8 Encoding	1
Stream Signature Violation	1
IP - Too Small TTL	1
Unauthorized Access to Service	2
Malformed HTTP Header Line	1

- Предустановленные отчеты
- Пользовательские отчеты
- Отчеты в соответствии со стандартами PCI, SOX and HIPAA
- Отчеты по требованию или по расписанию
- Формат HTML, PDF и RTF

iMPERVA®

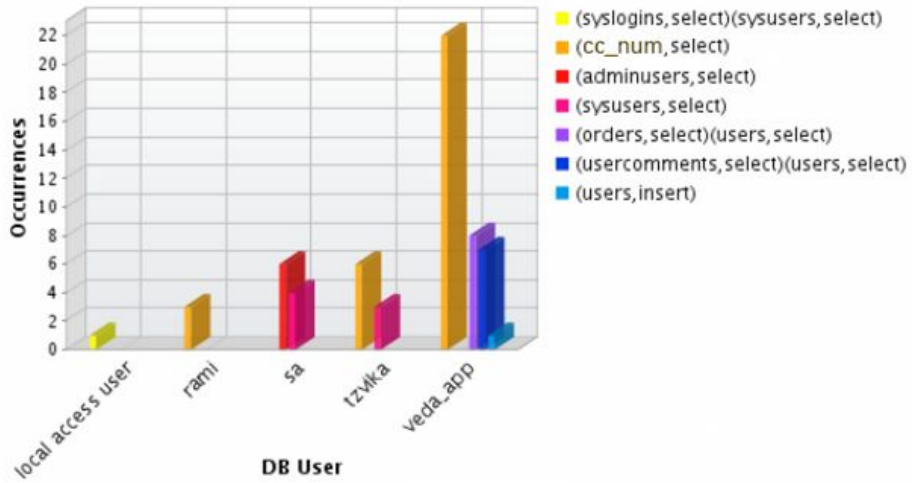
Графические отчеты

Sensitive Data - Private

Sensitive Data Private - Weekly (auditdata)

iMPERVA SECURESPHERE™

Graphical View



Detailed View

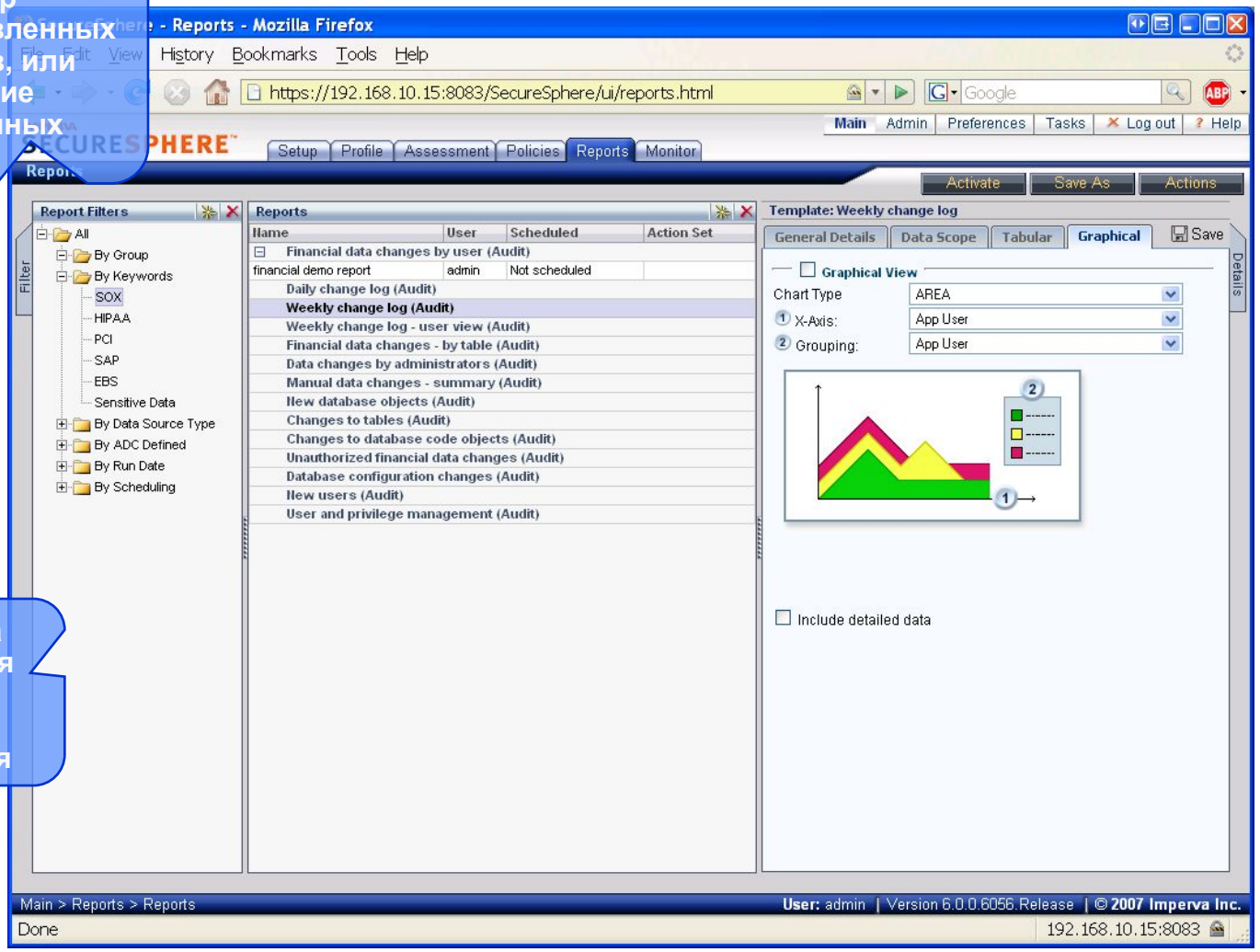
DB User	Query Group	Occurrences
veda_app	(cc_num,select)	22
tzvika	(users,select)	6
rami	(users,select)	3
sa	(sysusers,select)	4
sa	(adminusers,select)	6
veda_app	(orders,select)(users,select)	8
local access user	(syslogins,select)(sysusers,select)	1

iMPERVA®

Графические отчеты

Выбор предустановленных шаблонов, или создание собственных

Выбор вариантов представления отчета

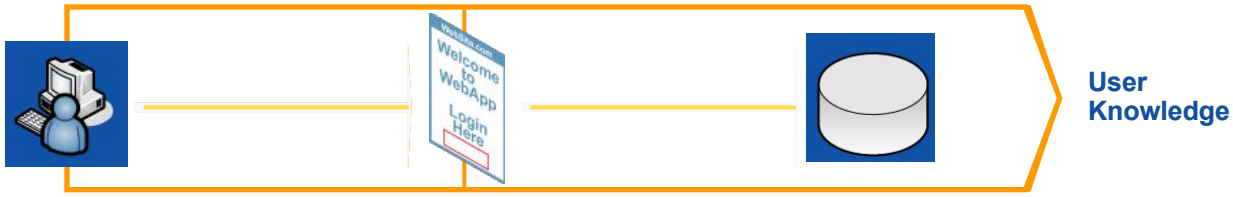


Настройка содержания отчета и создание расписания

IMPERVA

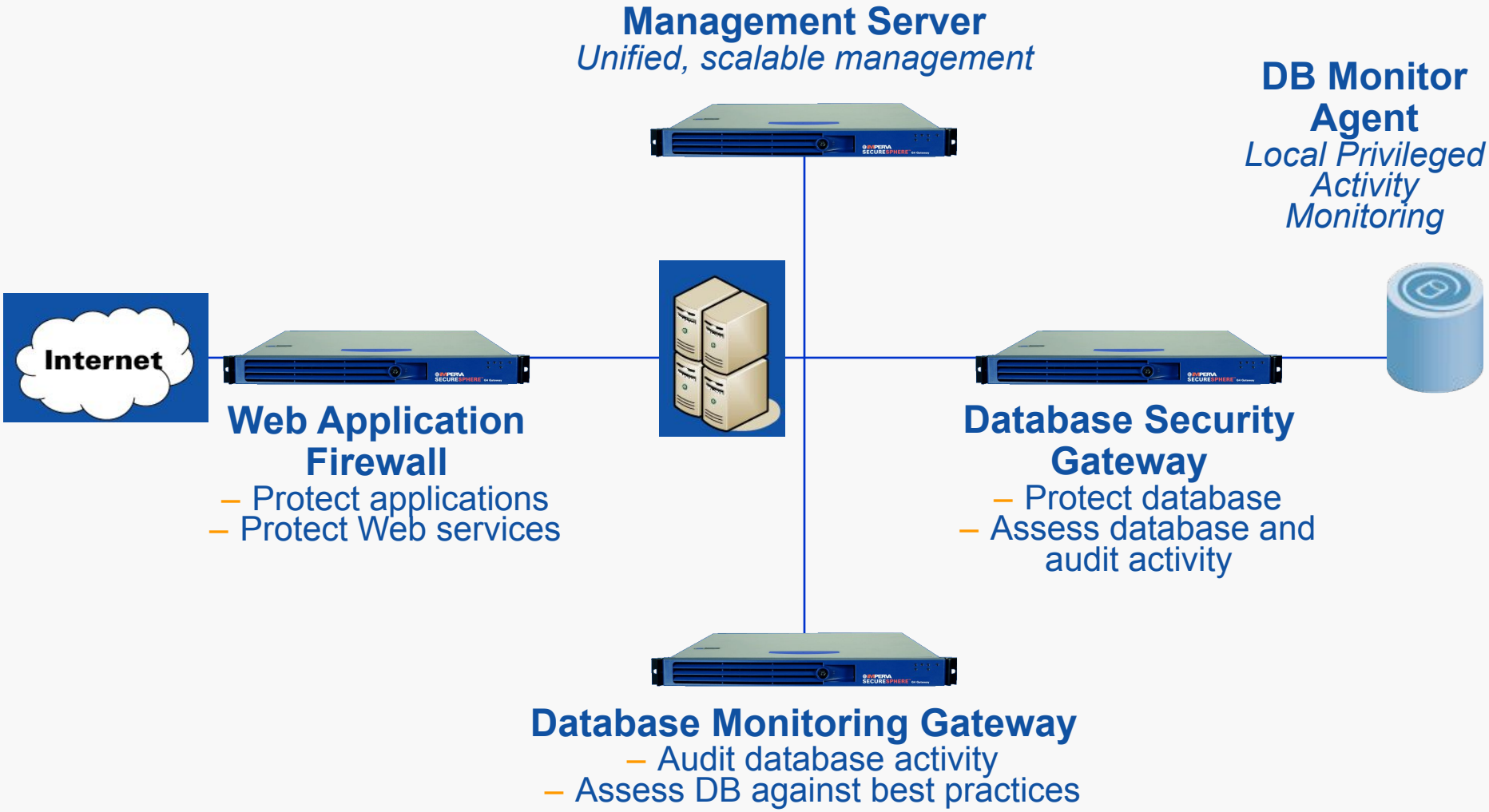
Мониторинг запросов web-пользователей (Universal User Tracking)

- Все запросы web-пользователей осуществляются от имени одной учетной записи (Connection pooling)
- С помощью журнала запросов на сервере БД возможно лишь понять, что доступ к данным был осуществлен от имени приложения



- SecureSphere осуществляет аудит SQL запросов от имени приложения
- С помощью SecureSphere могут быть идентифицированы web-пользователи

Продуктовая линейка SecureSphere



Технические характеристики Imperva SecureSphere

Модель	G4	G8/Crossbeam	G16 FTL
Пропускная способность	500MB/Sec	1GB/Sec	2GB/Sec
Скорость обработки транзакций, транзакций/с	16,000	24,000	36,000
Рекомендуемое число защищаемых Web-серверов	50	100	200
Форм-фактор	1U FTL Model: 2U	1U FTL Model: 2U	2U
Режим развертывания	Bridge, Router, Proxy or Monitor	Bridge, Router, Proxy or Monitor	Bridge, Router, Proxy or Monitor
Число защищаемых сегментов в режиме Bridge	2	2	2
Число интерфейсов в режиме Routing	5	5	5
Максимальное число интерфейсов управления	1	1	1
Функции высокой доступности	Fail Open, IMPVHA, VRRP	Fail Open, IMPVHA, VRRP	Fail Open, IMPVHA, VRRP

Почему Imperva?

Релевантные для бизнеса отчеты	Возможность генерации отчетов различной формы
Автоматизация и точность	Выявление изменений параметров приложений и поведения пользователей
Мониторинг всех каналов доступа к данным	Предоставление полной и достоверной информации для проведения аудита
Производительность и масштабирование	Высокая готовность и простота управления. Различные режимы развертывания
Сервис мирового уровня	Глобальная поддержка пользователей в режиме 24 X 7 X 365

Сервисная поддержка

- Компания обеспечивает всестороннюю поддержку пользователей, включая:
  - Возможность обращения по телефону или e-mail в режиме 24 x 7 x 365
  - Стандартная или авансовая замена оборудования
  - Online технический портал
- Профессиональные сервисы для тренинга и инсталляции

Виды сервисной поддержки

Support Level	Standard	Enhanced	Premium
Term	1 year	1 year	1 year
Support hours	8am - 6pm local time	24 x 7 x 365	24 x 7 x 365
Software maintenance	Full (major and minor updates)	Full (major and minor updates)	Full (major and minor updates)
Hardware warranty	Extended for term	Extended for term	Extended for term
Hardware replacement	Standard Replacement	Standard Replacement	Advance Replacement
Access to Imperva Self Service Support Portal	Yes	Yes	Yes

Тренинги от Imperva

- Виды тренингов:
  - On-Site Training
  - SecureSphere Training Class @ Imperva Offices
- Расписание уточняется через локальных представителей
- Транспортные расходы и проживание оплачиваются отдельно

Спасибо!

IMPERVA®