Обзор IBM Security Virtual Server Protection for VMware

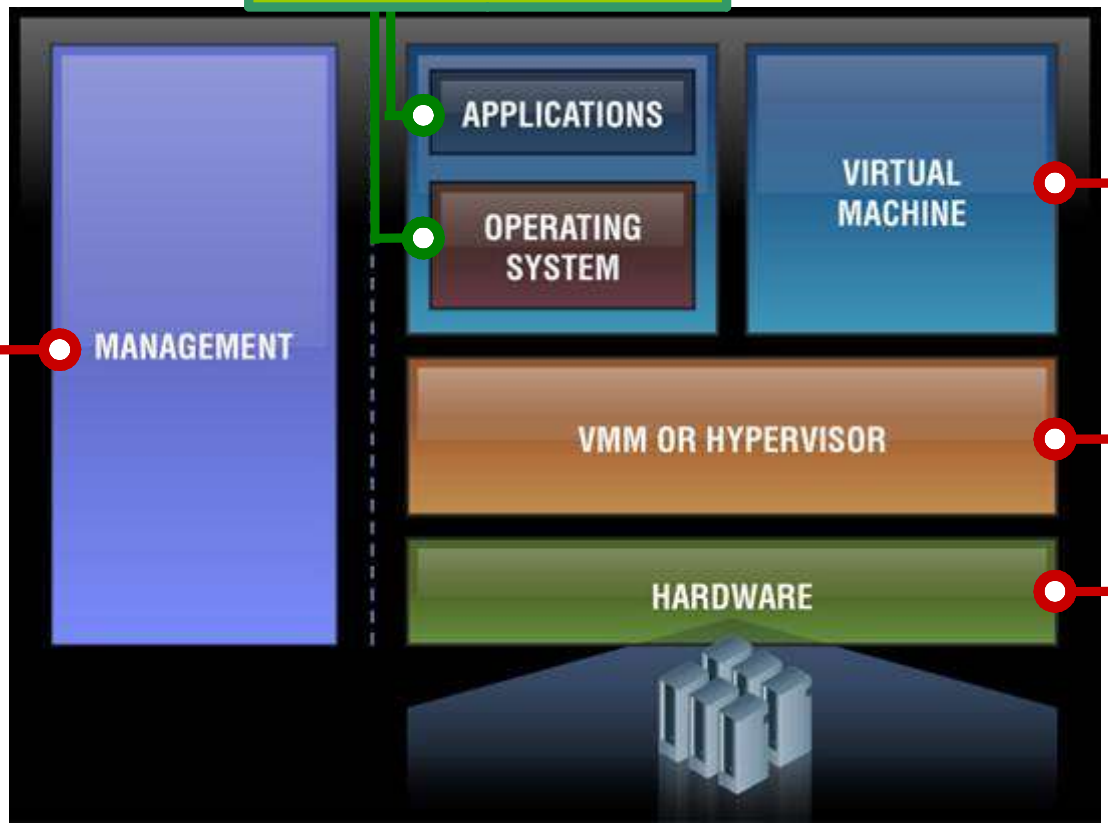
Кирилл Керценбаум

Kirill.Kertsenbaum@ru.ibm.com

Больше компонент = Больше угроз и больше сложностей для поддержки соответствия стандартам и требованиям

- **Традиционные угрозы**
- **Новые угрозы для Виртуальной среды**

Традиционные угрозы могут атаковать ВМ только как физические системы



Управление уязвимостями

Безопасность хранилищ служебных и программных данных

Требует новых навыков

Беспорядочное разрастание

Динамическое перераспределение

Захват ВМ

Распределение ресурсов

Единая точка отказа

Невидимые Руткиты на аппаратном уровне

Вирт. NICи и Ресурсы теперь мишень

Использование средств безопасности физической среды для виртуальной добавляет стоимость и сложность управления

Безопасность виртуализации от IBM

Решения по безопасности систем виртуализации от IBM включают программы и сервисы, оптимизированные для виртуальных сред, что позволяет ощущать преимущества от виртуализации при сохранение необходимого уровня безопасности

- Proventia® Server Intrusion Prevention System (IPS)
- Proventia Network IPS

- Proventia Virtualized Network Security Platform

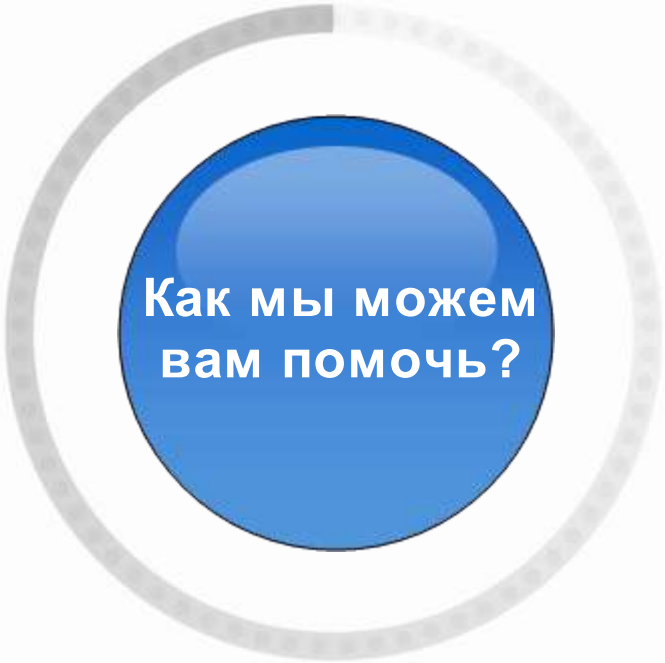
- **Virtual Server Protection for VMware**

IBM Security Virtual Server Protection for VMware позволяет обеспечить надежную защиту, соответствие требованиям и высокую отдачу

Интегрированная защита от угроз для платформы VMware vSphere

Помогает **соответствовать требованиям** обеспечивая безопасность и **отчетность** специально созданную для ВМ

Защищает и контролирует доступ к критическим данным на виртуальной инфраструктуре



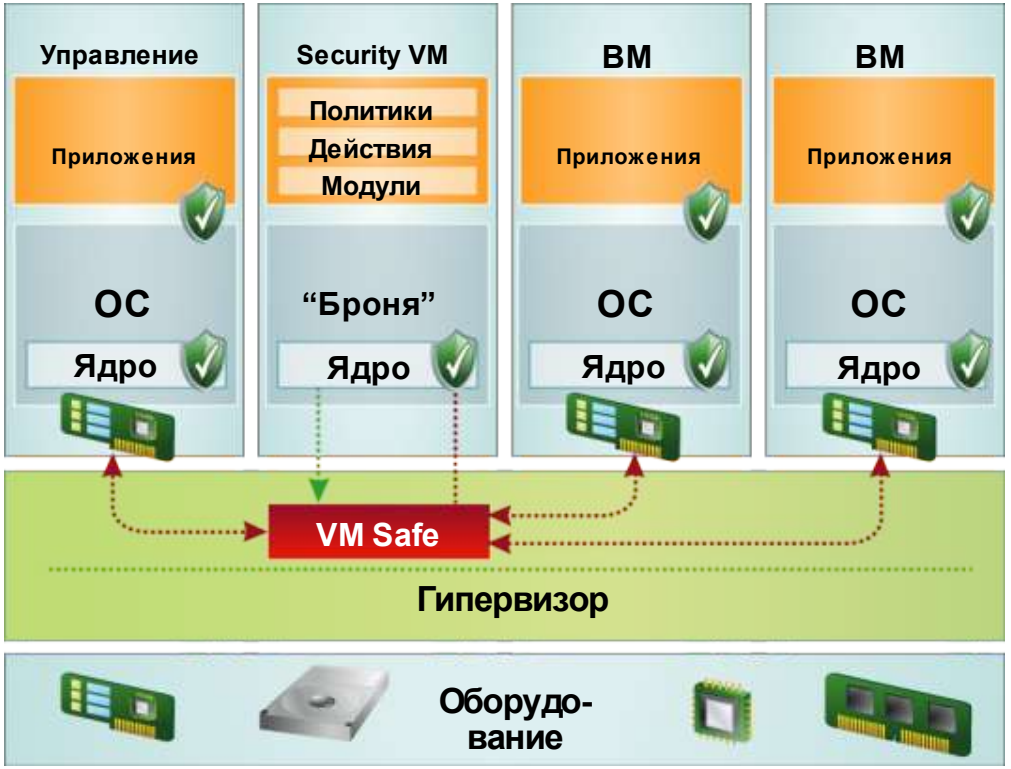
Создано для и **интегрировано** с виртуальной платформой

Увеличивает время безотказной работы и доступности с помощью механизма обнаружения Руткитов

Увеличение ROI с **динамической безопасностью и обнаружением ВМ**

Virtual Server Protection for VMware позволяет полностью ощутить преимущества виртуализации без снижения уровня Информационной безопасности

- Обеспечивает динамическую защиту для каждого уровня виртуальной инфраструктуры
  - Гипервизор
  - Хост
  - Сеть
  - Виртуальные машины (ВМ)
  - Внутренний ВМ трафик



Virtual Server Protection for VMware обеспечивает соблюдение лучших практик безопасности

1. **Процессы управления конфигурациями и изменениями должны быть расширены и включать Виртуальную инфраструктуру**
   - Автоматическое обнаружение и защита как только ВМ начинает работу
   - Внедрение в ОС хоста и виртуальную сеть для определения уязвимостей.
   - Технология IBM Virtual Patch® защищает от уязвимостей вне зависимости от стратегии обновлений
2. **Поддерживать раздельный контроль доступа несмотря на то, что сервера, сеть и инфраструктура безопасности теперь едины**
   - Контроль в виртуальной сети
     - Ограничение или запрет сетевого доступа от виртуального сервера до подтверждения политики безопасности
   - Мониторинг и отчетность по виртуальной инфраструктуре
3. **Обеспечивать разделение Виртуальных машин и Виртуальной сетевой инфраструктуры**
   - Изоляция ресурсов на сетевом уровне
4. **Поддержка аудита логов в Виртуальной среде**
   - Мониторинг и отчетность по виртуальной инфраструктуре

*Источник: RSA Security Brief: Security Compliance in a Virtual World http://www.rsa.com/solutions/technology/secure/wp/10393_VIRT_BRF_0809.pdf

Virtual Server Protection for VMware может ускорить и упростить аудит на соответствие PCI DSS и помочь ему соответствовать

- Обеспечивает сетевое разграничение для снижения объемов аудита
- Мониторит целостность критических систем
- Определяет и блокирует атаки, направленные на карточные данные
- Использует IBM Virtual Patch для закрытия уязвимостей вне зависимости от политики обновлений
- Собирает важные сведения об инцидентах на ВМ
- Изолирует процессинговые приложения на ВМ на одном и том же аппаратном обеспечении и от систем с карточными данными

В конце 2009 года PCI DSS добавил требования по безопасности Виртуализации

VSS помогает соответствовать Аспектам Безопасности стандарта PCI DSS

Требование 1 – Настройка Файрволов и Маршрутизаторов (для 1.1, 1.1.2, 1.2.1, 1.3.1, 1.3.2, 1.3.4, 1.3.5, 1.3.7 и 1.4.2)

Требование 2 – Стандарт Конфигураций (для 2.2, 2.2.1, 2.2.2 и 2.4)

Требование 6 – Политика обновлений (для 6.1, 6.2, 6.5 and 6.6)

Требование 10 – Мониторинг и слежение за доступом к данным (для 10, 10.2, 10.5.2, 10.5.5 и 10.6)

Virtual Server Protection for VMware увеличивает ROI от виртуальной инфраструктуры через использование безопасности уровня физических систем для виртуализации

- **Автоматическая защита для каждой работающей ВМ**
  - Автоматическое обнаружение
  - Автоматизированное управление поиском уязвимостей
  - IBM Virtual Patch®
- **Упрощенная**
  - Без перенастройки виртуальной сети
  - Без установки на гостевые ОС
    - –Улучшенная стабильность
    - –Больше свободных ресурсов
    - –Сниженная площадь атаки
- **Защита для любой гостевой ОС**
  - Нет необходимости агентов для различных ОС
- **Минимальное присутствие на гостевой ОС**
  - Улучшенная стабильность
  - Больше свободных ресурсов
  - Сниженная площадь атаки
- **Упрощенное управление снижает количество административных задач**
  - Одна Security Virtual Machine (SVM) на физический сервер
  - Защита 1 к многим
  - Интенсивные затраты CPU удалены с гостевых ОС и сосредоточены на SVM
- **Централизованное управление**
  - IBM Proventia® Management SiteProtector

Почему решение по безопасности виртуализации от IBM?

Только IBM предлагает сочетание продуктов и услуг от одного вендора необходимых для любой организации, желающей оценить все преимущества виртуализации с сохранением высокого уровня защиты информации

1. *Снижение стоимости **применения новейшей экспертизы безопасности виртуализации**, процессов и технологий*
2. ***Снижение риска**, мониторинг и управление новейшими **угрозами и безопасности***
3. *Определение и снижение рисков виртуализации в части **несоответствия требованиям***
4. *Снижение расходов за счет **ограничения внутреннего доступа** к ВМ и внешнего использования **важной информации***
5. *Снижение стоимости **управления правами и доступом***
6. *Контроль увеличивающегося риска **уязвимостей на уровне приложений***

Целый спектр требований и технологий необходим для безопасности Виртуальной инфраструктуры

Конечный пользователь

Привилегии доступа пользователей
централизованный доступ и аудит политик, каталогов

Управление Ролями
single sign-on, технология предоставления

Управление привилегиями пользователей
изменение процессов контроля для привилегированных пользователей

Доверенные роли
защита данных работников и клиентов

Люди и Доступ

Администратор

Изоляция данных
шифрование, разделение сетей, Оборудования / ОС / Прил. / БД

Восстановление данных
бэкап, удаленное хранилище

Сокращение и удаление данных
безопасный процесс удаления данных клиентов и служебной информации

Защита от утечек данных
Технология DLP для хранимой и перемещаемой информации

Данные и Информация

Аудитор

Аудит и требования
аудит создания политик, логов и управления

Поддержка расследований
хранение, поиск и корреляция данных аудита

Управление политиками
унифицированная безопасность, распространение политик

Безопасное выделение ресурсов
управление образами, политики общего доступа

Тестирование приложений
управление уязвимостями

Приложения и Процессы

Разработчик

Безопасность серверов
аудит, контроль доступа

Сетевая безопасность
Firewall, IPS, VLAN

Безопасность виртуализации
Сегментация ВМ, Виртуальные решения, Интегрированная безопасность Гипервизора

Защита браузеров
ssl, защита памяти, антивирус

Управление обновлениями
приоритезация, расписание, сбор данных

Сеть, Сервер и ПК

Провайдер сервисов

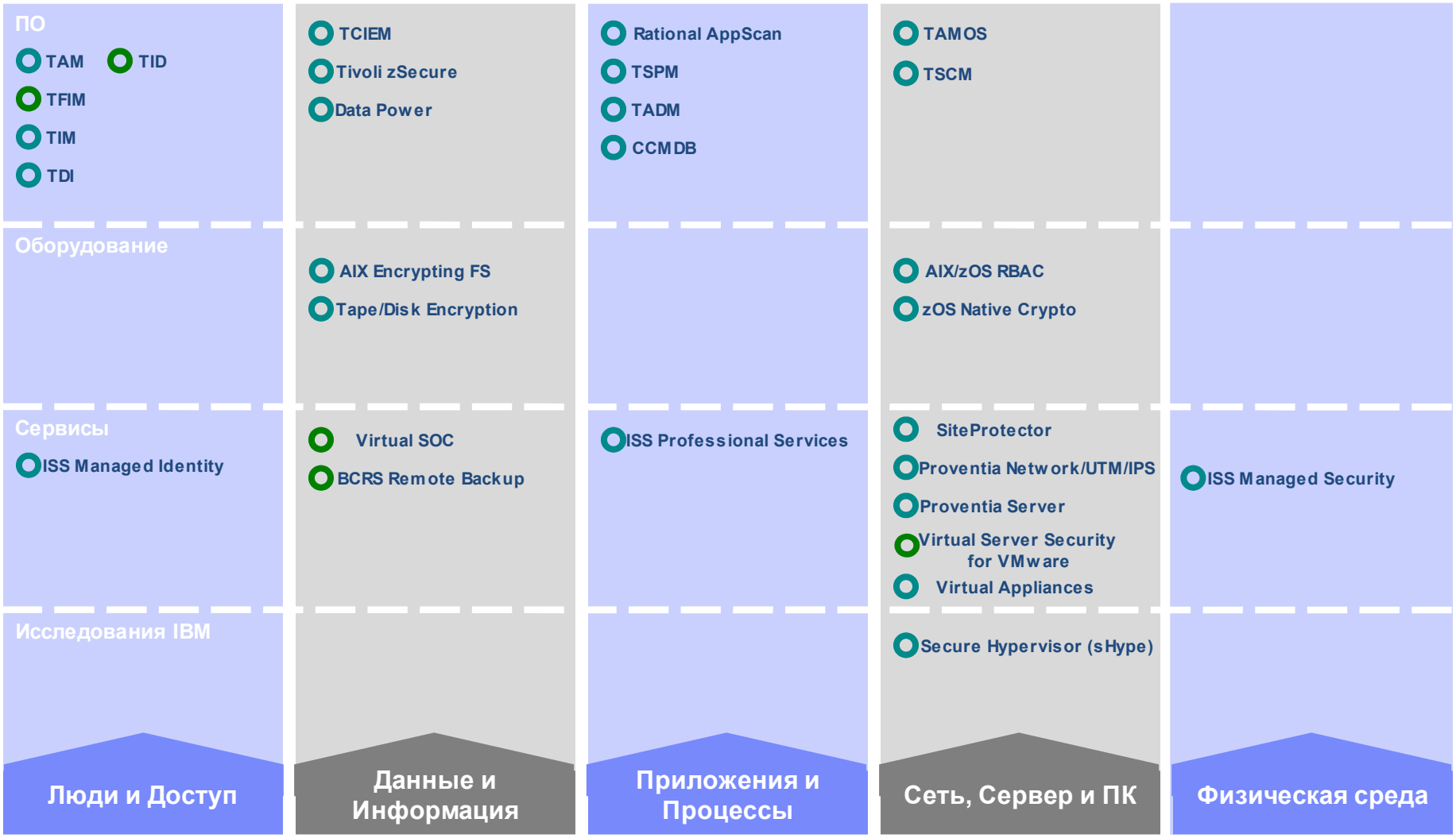
Нахождение данных
“облачные” дата центры

Катастрофоустой-чивость
“эластичные облака”

Доступность
географическое распределение нагрузки

Физическая среда

Технологии безопасности IBM для виртуализации



IBM Security Virtual Server Protection for VMware

Интегрированная защита для VMware vSphere™ 4

Помогает быть более эффективными, соответствовать требованиям и уровню безопасности с помощью интегрированной и оптимизированной безопасности для виртуальных дата центров:

- Помогает соответствовать стандартам и требованиям безопасности
- Специально создано и полностью интегрировано с VMware
- Защищает и следит за доступом к важной информации
- Повышает надежность и доступность Виртуальной инфраструктуры
- Увеличивает ROI через динамически расширяемую систему защиты

- Межсетевое экранирование и Система Предотвращения вторжений
- Защита от Руткитов
- Анализ трафика внутри ВМ
- Интеграция на уровне Гипервизора (VMsafe)
- Автоматическая защита для мобильных ВМ (VMotion)
- Защита сегментов виртуальной сети
- Защита на уровне виртуальных подсетей
- Аудит виртуальной инфраструктуры (Привилегии пользователей)
- Контроль доступа к виртуальной сети

СПАСИБО!