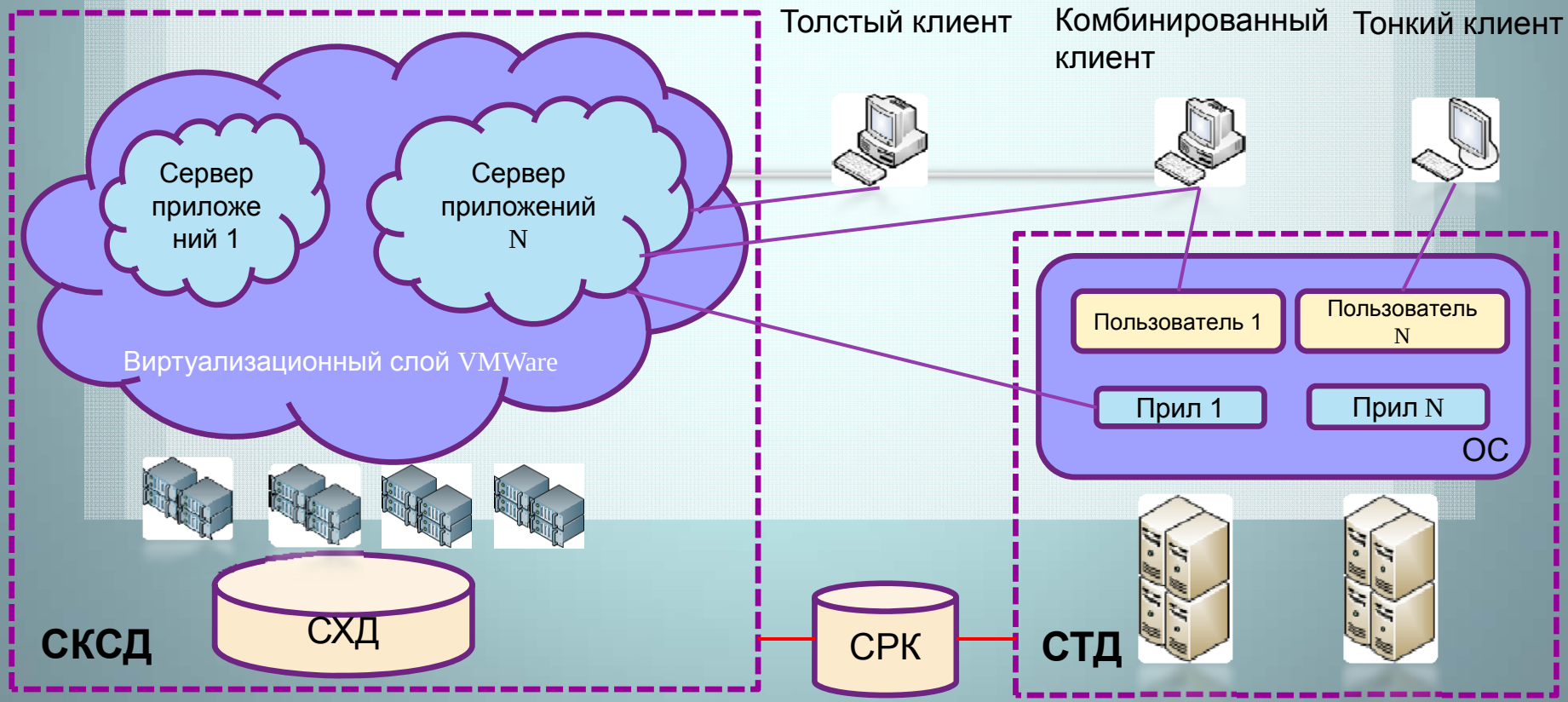
Макет облачной инфраструктуры

Шибаев Александр,
МЦИ Банка России

Унифицированные решения Банка России

Основа территориального центра обработки – типовые проектные решения:

- Система консолидированных серверов и данных
- Система терминального доступа
- Система резервного копирования



Результаты внедрения систем виртуальных серверов и терминального доступа в Банке России

Внедрения проекта виртуальных серверов в учреждениях Банка России позволило:

- сократить времени на внедрение автоматизированных систем

(подготовка технической базы автоматизированной системы с 4-5 месяцев до 2-3-дней);

- снизить стоимости владения комплексом технических средств;
- повысить надежности за счет свойств виртуальной среды и резервирования;
- повысить эффективное использование вычислительных ресурсов (с 1-5% до 50-80%);
- снизить затраты на администрирование комплекса серверов;
- по мере роста потребностей проводить модернизацию СКСД, а не АС;
- экономить площади ВЦ (около 100 виртуальных серверов и рабочих станций – 1 стойка);
- снизить требования к системам инженерного обеспечения.

Внедрение проекта СТД в территориальных управлениях позволило :

- отказаться от серверного оборудования в РКЦ (в ИС);
- снизить трудоемкость администрирования типовых программных комплексов;
- сократить время на внедрение ППК;
- снизить стоимость АРМ ТУ.

Развитие СКСД и СТД

- повышение управляемости существующей инфраструктуры
- автоматизация процессов администрирования
- обеспечение непрерывности процесса предоставления сервисов и повышение их качественных характеристик
- повышение показателей быстродействия и качества обслуживания инфраструктуры
- повышение уровня информационной безопасности
- обеспечение оперативной эластичности (масштабируемости)
- Использование виртуальных рабочих мест пользователей (VDI)

Цели создания макета облачной инфраструктуры

- ✓ **Снижение затрат:**
  - Снижение количества персонала, обслуживающего ИС, выполняющего тот же объем работ
- ✓ **Повышение качества обслуживания:**
  - Сокращение числа и вероятности допущения ошибок при выполнении работ обслуживающим ИС персоналом;
  - Обеспечение высоких значений отказоустойчивости и доступности предоставляемых сервисов;
  - Тотальный контроль и управление элементами физической и виртуальной инфраструктуры
- ✓ **Сокращение времени выполнения заявок:**
  - Сокращение времени и затрат на обработку типовых запросов на обслуживание

Решения, рассматриваемые при подготовке макета

Обзор облачных решений

Поставщики облачных решений

	HP CSA	BMC BladeLogic	DELL VIS	Vmware vCloud Director	IBM CloudBurst
Поддержка компонент сторонних разработчиков		П	П		
Интегрированное решение	П			П	П
Быстрое и удобное создание сервисов					
Управление жизненным циклом приложений	П	П	П		
Контроль потребляемых сервисов	П	П		П	П
Решение для частного «облака»	П	П	П	П	П
Инсталляция приложений	П	П	П		П
Конфигурирование серверов	П	Нет управления СХД	Не интегрированное решение	П	П

Задачи для отработки на макете облачной инфраструктуры

- Практическая проверка общих принципов построения и управления облачной инфраструктурой
- Отработка контролируемого централизованного предоставления пользователям набора ИТ- сервисов
- Проверка возможности администрирования всего комплекса сокращенным обслуживающим персоналом - до 500 контролируемых ресурсов на 1-ого сотрудника и повышение качества их обслуживания
- Тестирование решений информационной безопасности облачной инфраструктуры

Макет облачной инфраструктуры

В рамках Макета под понятием «облако» понимается совокупность следующих элементов:

- Система консолидированных серверов обработки и хранения данных в составе:
  - 3-х серверов виртуализации (HP BL460)
  - сервера управления (HP DL360)
  - системы хранения данных (EMC CLARiiON)
- Установленный на СКСД комплекс программного обеспечения управления и автоматизации администрирования виртуальных серверов:
  - программные средства виртуализации (VMWare ESXi, vCenter Server)
  - программные средства контроля и управления виртуальной инфраструктурой (HP CSA, Operations Orchestration, Server Automation)
- Специализированные программные средства для обеспечения информационной безопасности (ИБ) в виртуальной среде:
  - централизованной антивирусной защиты
  - централизованного контроля и управления событиями ИБ - разграничение доступа, контроль целостности, разделение полномочий в виртуальной среде и др.

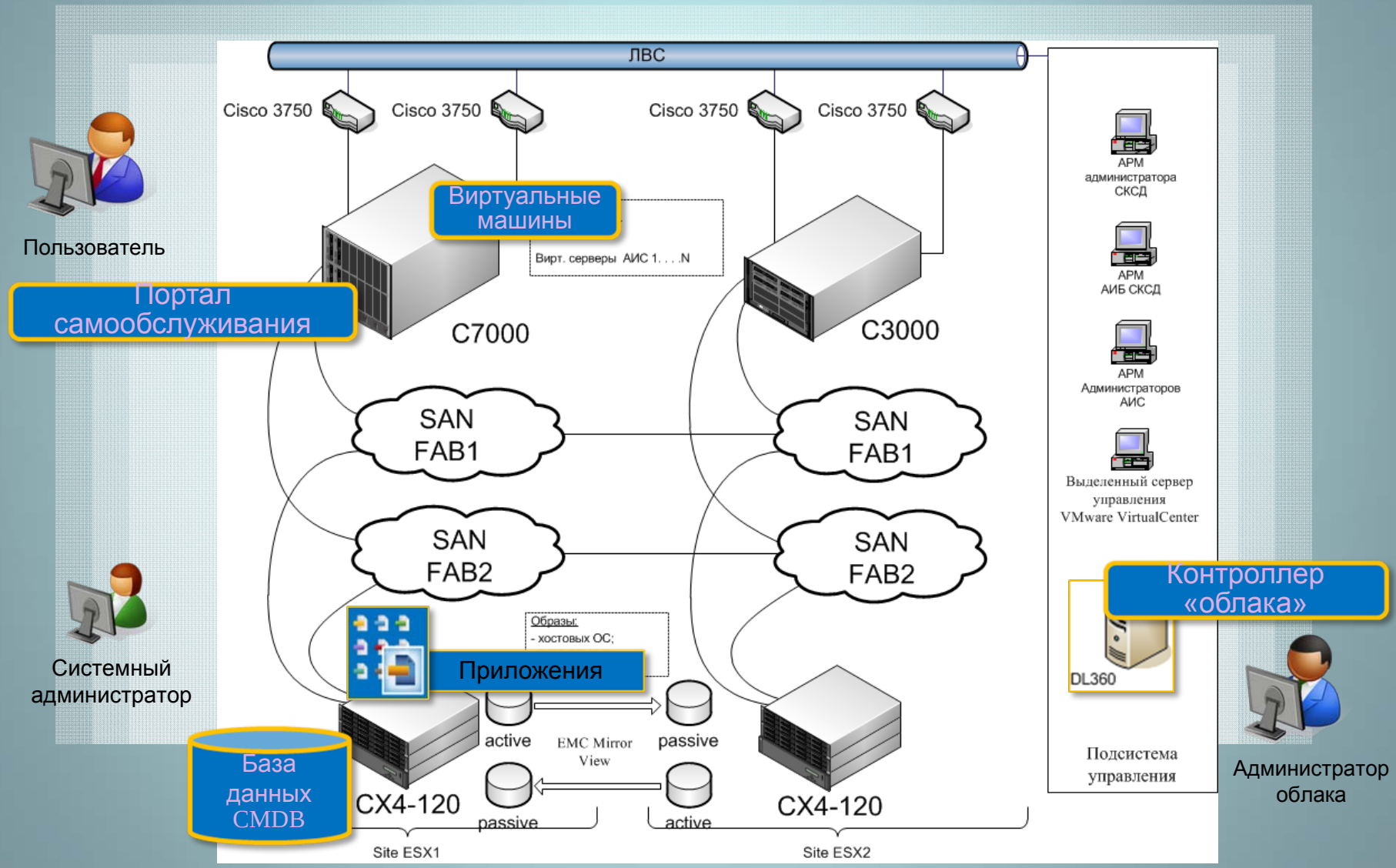
Функциональность макета для целевой аудитории

- ✓ **Системные операторы и администраторы**
  - предоставление платформы для развертывания серверных инфраструктур и рабочих мест пользователей
  - предоставление инструментов контроля и управления
- ✓ **Администраторы систем облака**
  - консолидация рабочих мест операторов АС
  - консолидация рабочих мест администраторов АС
- **Выделение типовых рабочих мест администраторов подсистем облака:**
  - АРМ администратора облачной инфраструктуры
  - АРМ администратора средств защиты от вредоносного кода
  - АРМ администратора информационной безопасности

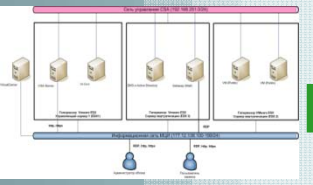
Обзор облачных решений

Решение HP Cloud Service Automation

Макет облачной инфраструктуры на базе СКСД МЦИ



Развитие макета облачной инфраструктуры



Администратор облака

RDP, http, https

Сеть управления CSA (192.168.251.0/24)

CSA Server

SA Core

VirtualCenter

DNS и Active Directory

Gateway (Mail)

Гипервизор Vmware ESX
Управляющий сервер 1 (ESX1)

VM (Public)

VM (Public)

Гипервизор VMware ESX
Сервер виртуализации (ESX 2)

VM (Public)

VM (Public)

Гипервизор Vmware ESX
Сервер виртуализации (ESX 3)

http, https

Информационная сеть МЦИ (177.12.138.100-199/24)

RDP, http, https

Пользователь
сервиса

Уязвимости облачной среды

- Отсутствие защиты гипервизора
- Отсутствие контроля действий пользователей и вносимых ими изменений в конфигурацию виртуальной среды
- Отсутствие требуемого уровня защиты виртуальных машин, долгое время находящихся в выключенном состоянии
- Отсутствие межсетевых экранов в виртуальной среде
- Опасность перегрузки вычислительных ресурсов при использовании стандартных средств защиты от вредоносного кода

Опасности облачной среды

- получение несанкционированного управления системой виртуальных серверов
- несанкционированный доступ к виртуальным машинам
- внедрение вредоносного ПО при работе пользователей на персональном виртуальном компьютере
- несанкционированный сетевой доступ внутри виртуальной инфраструктуры
- несанкционированное изменение виртуальных машин в выключенном состоянии
- угроза компрометации образов виртуальных машин

Угрозы информационной безопасности в облаке

Атаки между виртуальными машинами

VM VM VM VM VM

Активные

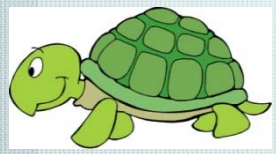
Проснулись, но системы безопасности устарел

Спящие виртуальные машины

VM VM VM VM VM VM

Разные уровни безопасности для данных

VM VM VM VM VM

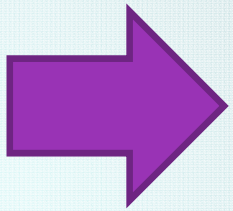


VM VM VM VM VM

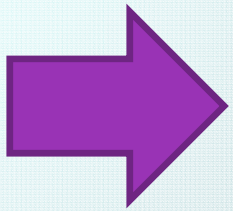
Обычный антивирус

Выбранные решения проблем информационной безопасности

- Отсутствие защиты гипервизора
- Отсутствие контроля действий пользователей и вносимых ими изменений в конфигурацию виртуальной среды



- Отсутствие требуемого уровня защиты виртуальных машин, долгое время находящихся в выключенном состоянии
- Отсутствие межсетевых экранов в виртуальной среде
- Опасность перегрузки вычислительных ресурсов при использовании стандартных средств защиты от вредоносного кода



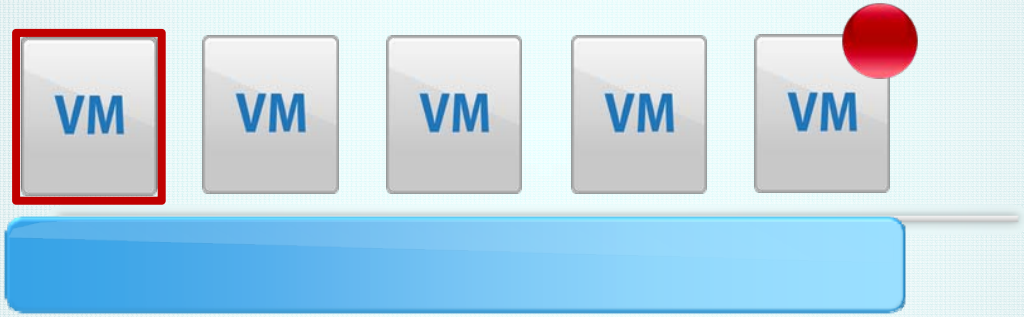
Trend Micro Deep Security

Решение Trend Micro Deep Security

Virtual Appliance:
- AV, IDS/IPS, FW
- высокая эффективность
- управляемость

Координированный подход:
- Оптимизированная защита

Агенты безопасности:
- Дополнительные модули защить
- Мобильность для перемещения в облако



Интеграция с гипервизором и vCenter:
- Понимается контекст виртуализации
- Защищает машины при включении

Макет облачной инфраструктуры

С точки зрения пользователей

- Стандартизированные услуги самообслуживания
- Быстрое предоставление услуг

С точки зрения администраторов

- Виртуализированные ресурсы
- Управление единым ресурсом
- Предоставление услуг с гибким масштабированием
- Автоматическая инсталляция, конфигурация и обновление приложений
- Единая консоль автоматизированного мониторинга и управления
- ✓ Бесконфликтное разделение зон ответственности с АИБ

Основные преимущества HyTrust HTA

- Отдельная консоль администратора ИБ
- Прозрачен для администратора облака
- Обеспечение контроля всех видов подключений к vCenter
- Обеспечение гибкого ролевого разграничения доступа к элементам управления облачной инфраструктуры
- Поддержка двухфакторной аутентификации
- Выдача привилегий на время

Основные преимущества Trend Micro Deep Security



Безопасность

Защищает от атак нулевого дня веб-приложения, корпоративные системы и ОС.

Обнаруживает и блокирует множество угроз.

ИТ-службы

Повышает степень консолидации виртуальных машин, одновременно снижая воздействие на производительность.

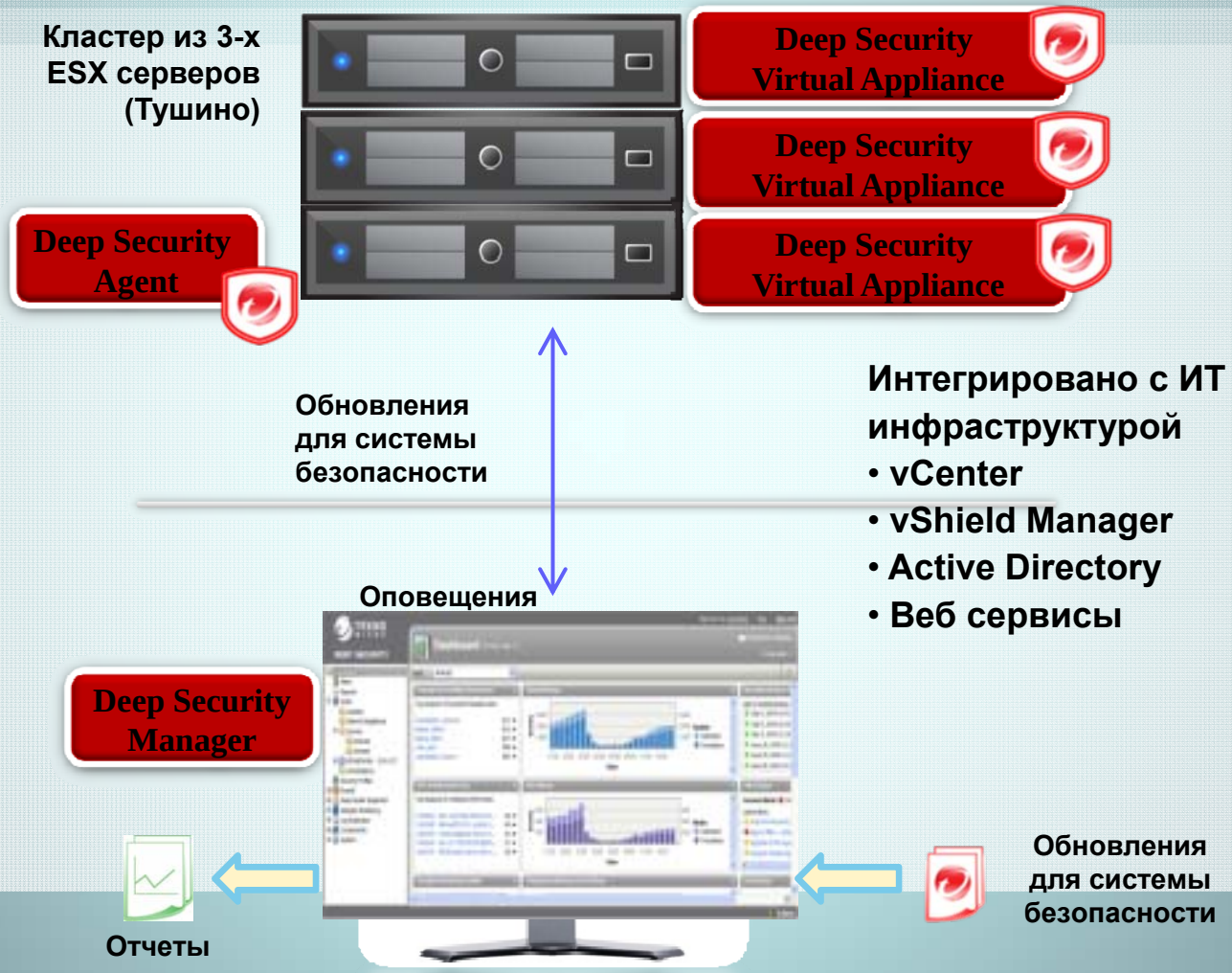
Более эффективный и быстрый патчинг.

Пользователи

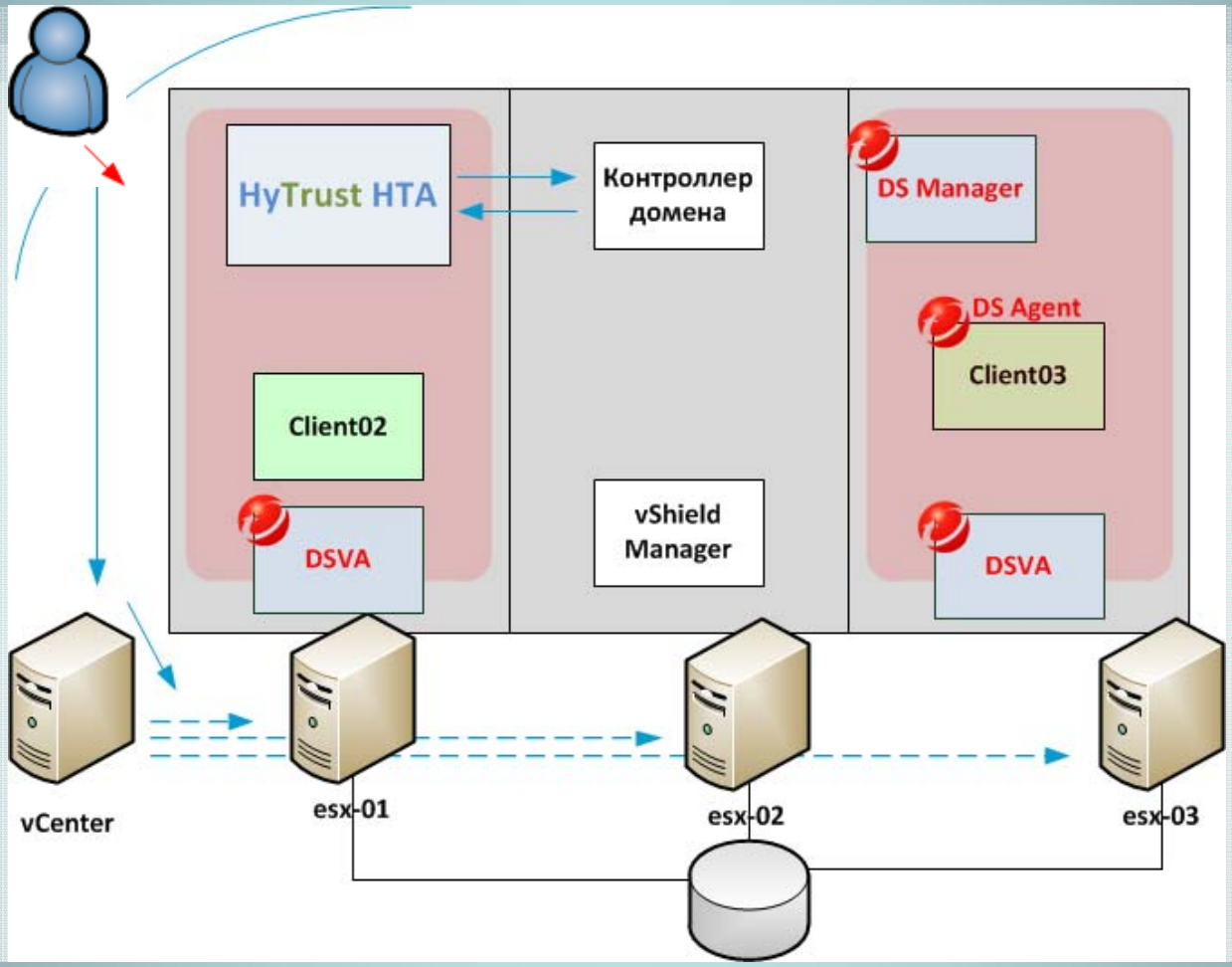
Избавляет от необходимости в агентах безопасности

Избавляет от необходимости осуществлять обновления

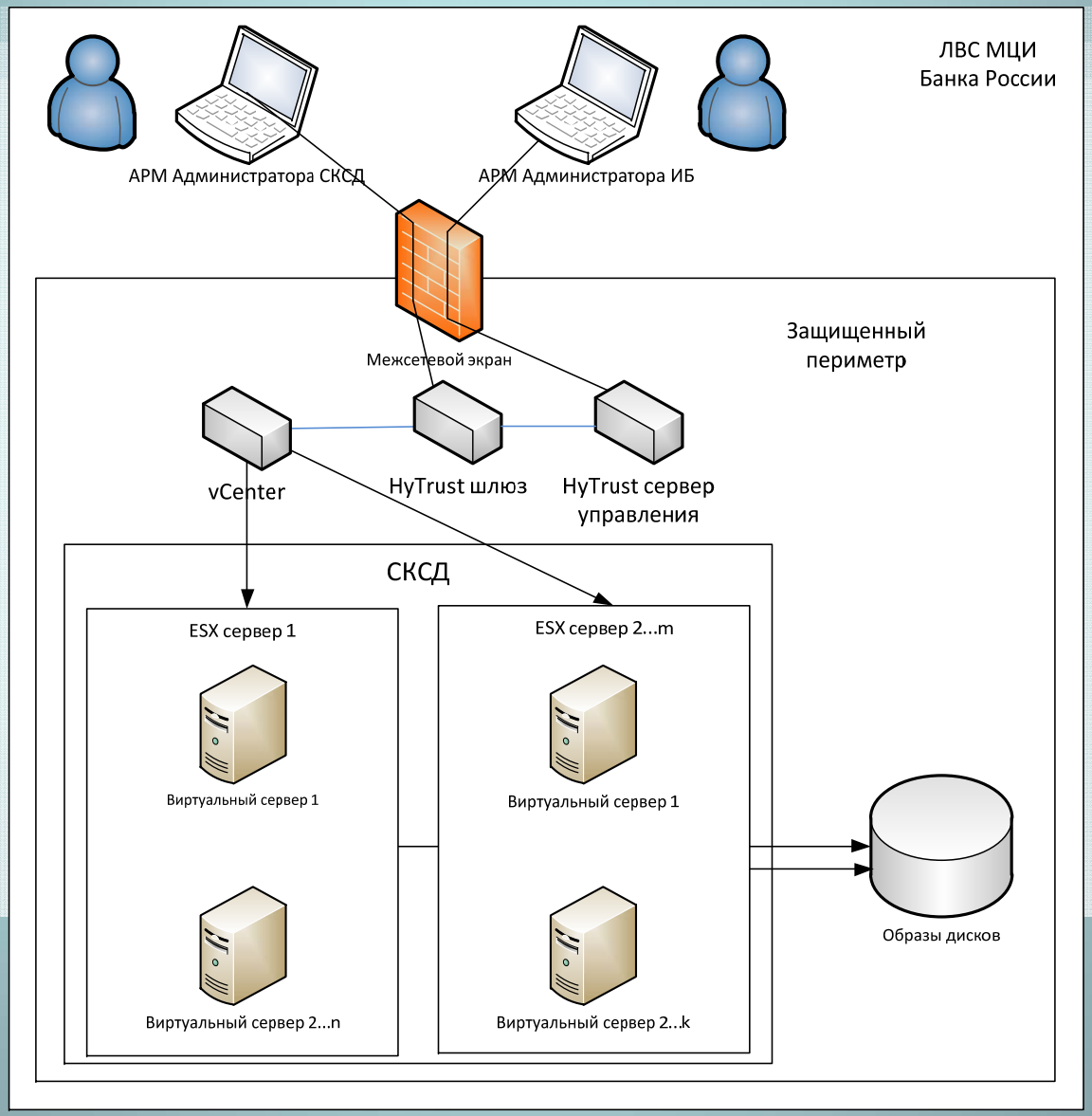
Архитектура макета



Текущая реализация защиты макета



Решение проблем ИБ с использованием HyTrust HTA



HyTrust HTA
консоль администратора

Разделение функциональных обязанностей

Пользователь

Администратор системы

АИБ агентов

АИБ системы

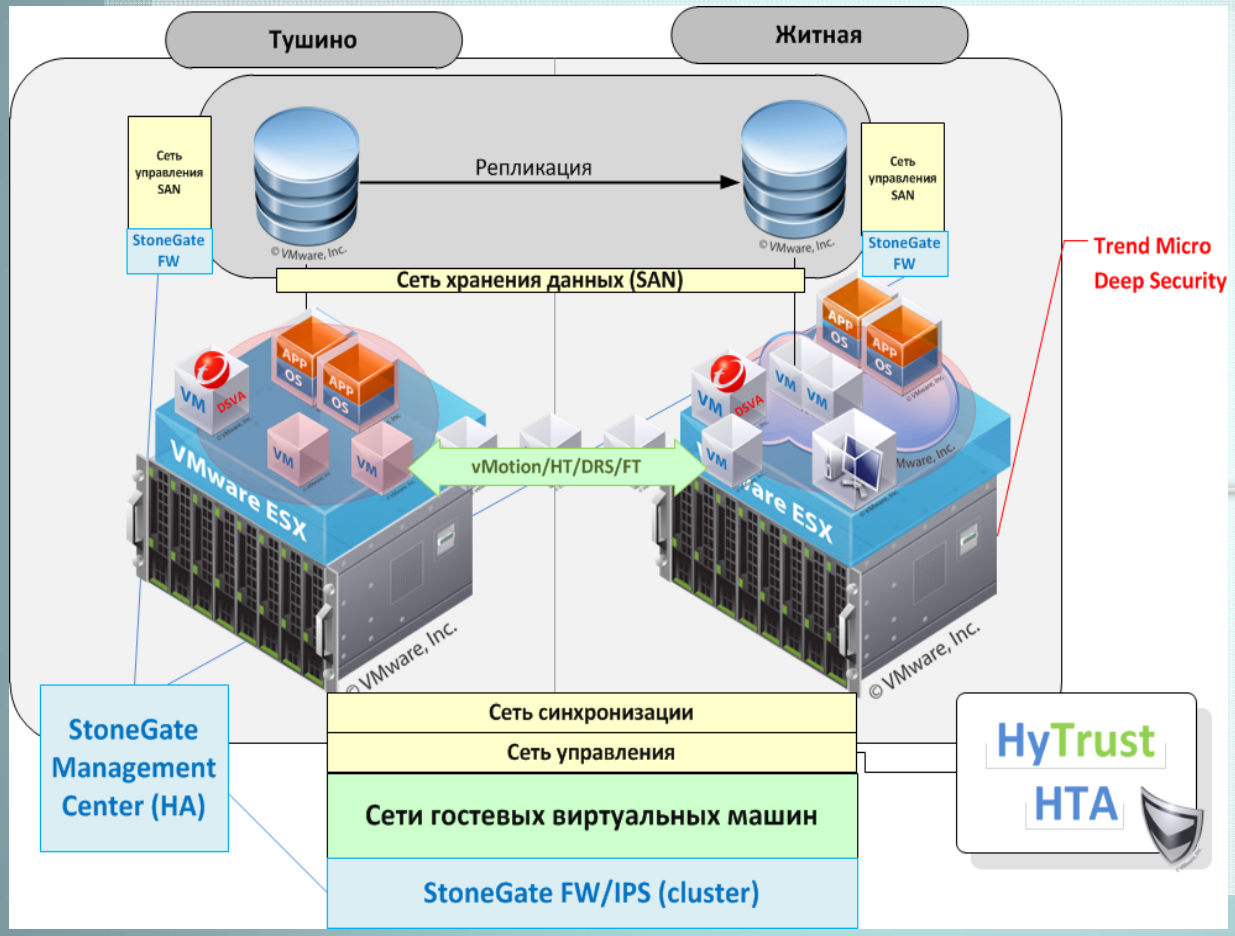
Виртуальная машина

HP CSA

Trend Micro Deep Security

HyTrust HTA

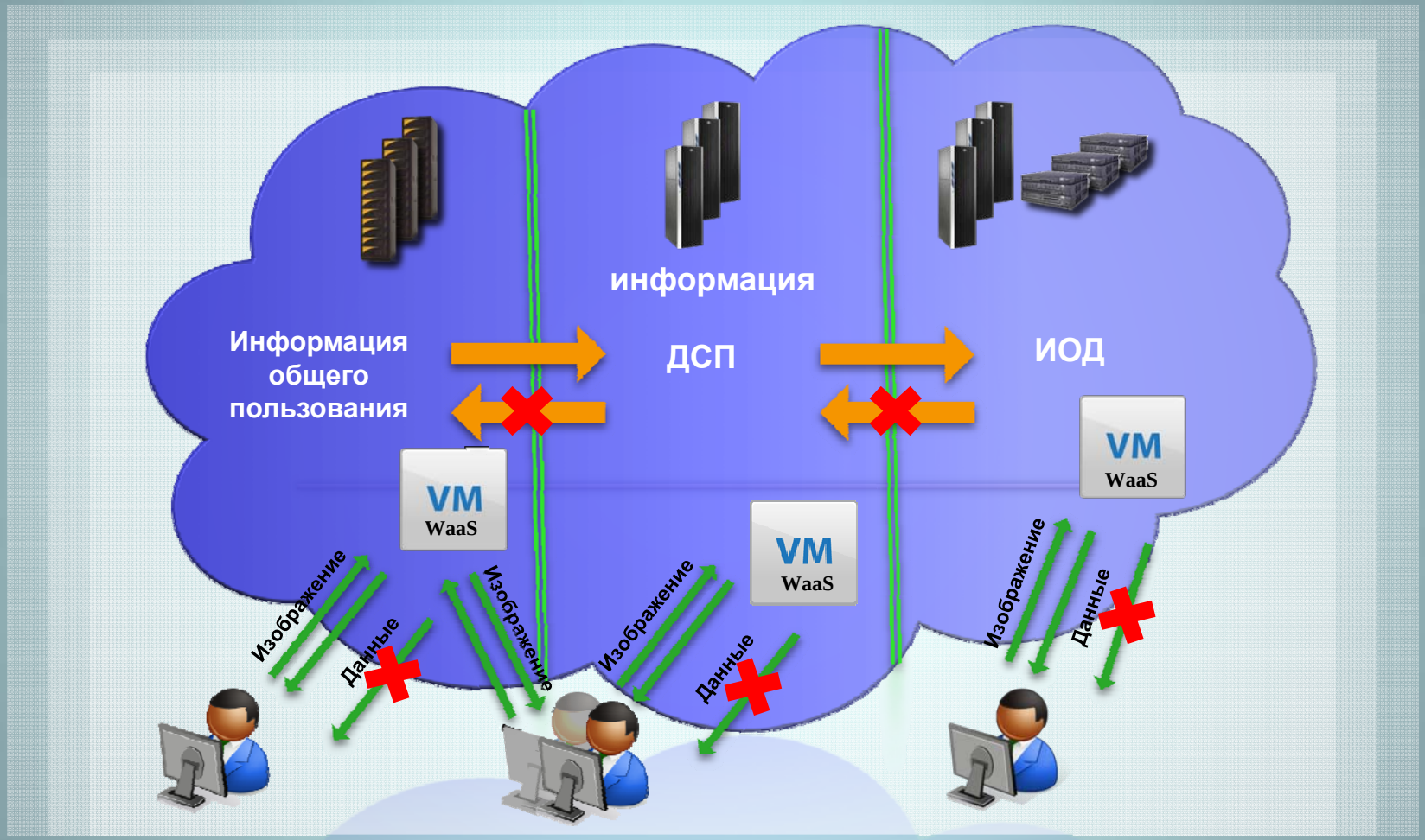
Рекомендации по защите облачной среды



- Контроль сетевых взаимодействий
- Антивирус без агентов
- Управление доступом к объектам ВИ
- Защита периметра виртуальной инфраструктуры
- Контроль доступа к средствам администрирования
- Управление событиями ИБ и их корреляция

Контроль доступа к данным в облачной среде

Зонирование информации по уровням безопасности



Спасибо за внимание!

Шибаев Александр,
МЦИ Банка России