Олег Летаев, Представитель по продажам IBM Security Solutions
3 Июнь, 2010

Обеспечение комплексной безопасности виртуальной среды – IBM Security Virtual Server Protection

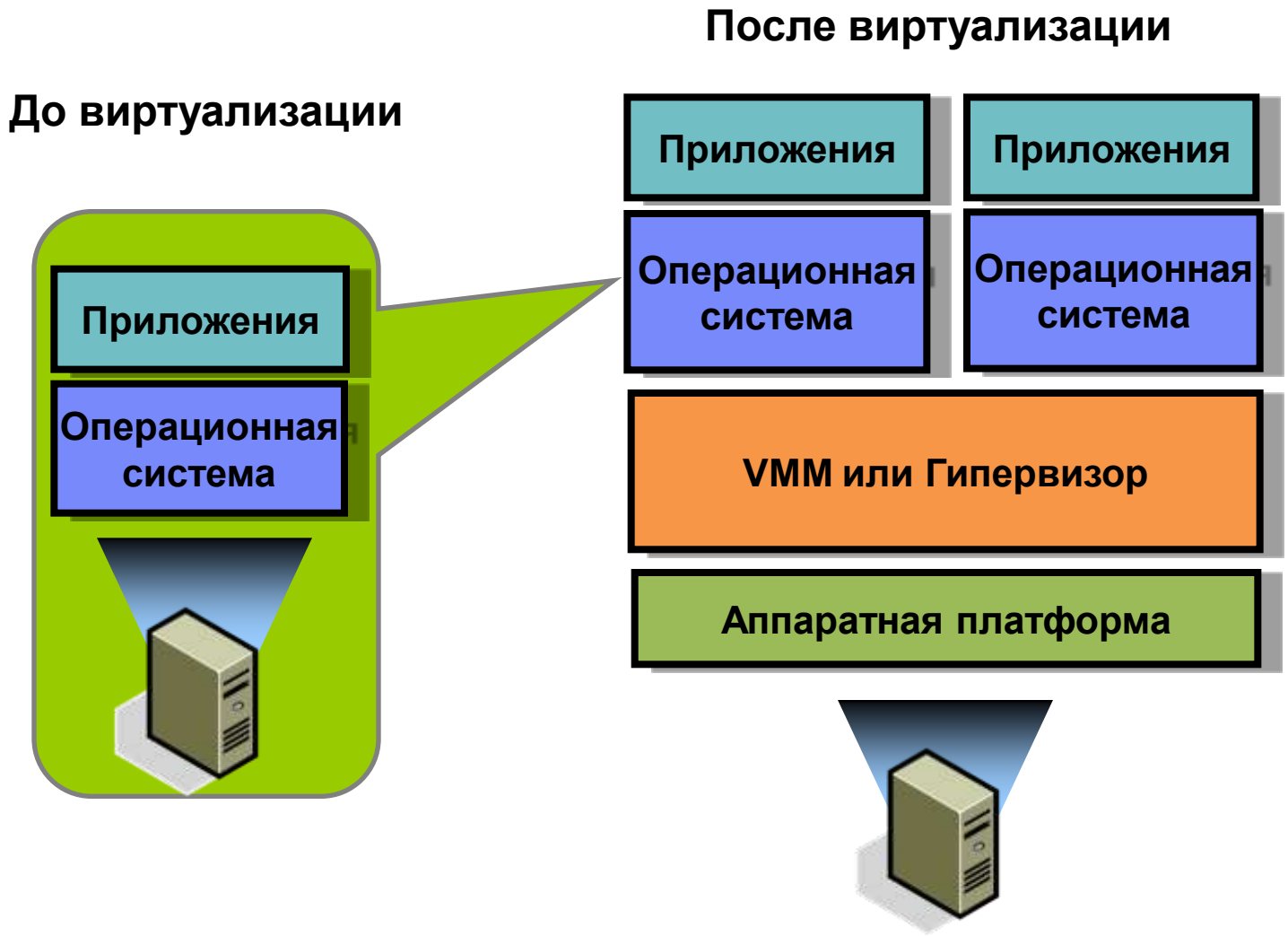
План

Виртуализация — новые технические риски

Виртуализация — новые организационные риски

Защита виртуальной инфраструктуры — IBM Security Virtual Server Protection

Архитектура виртуализации



Что меняет виртуализация?

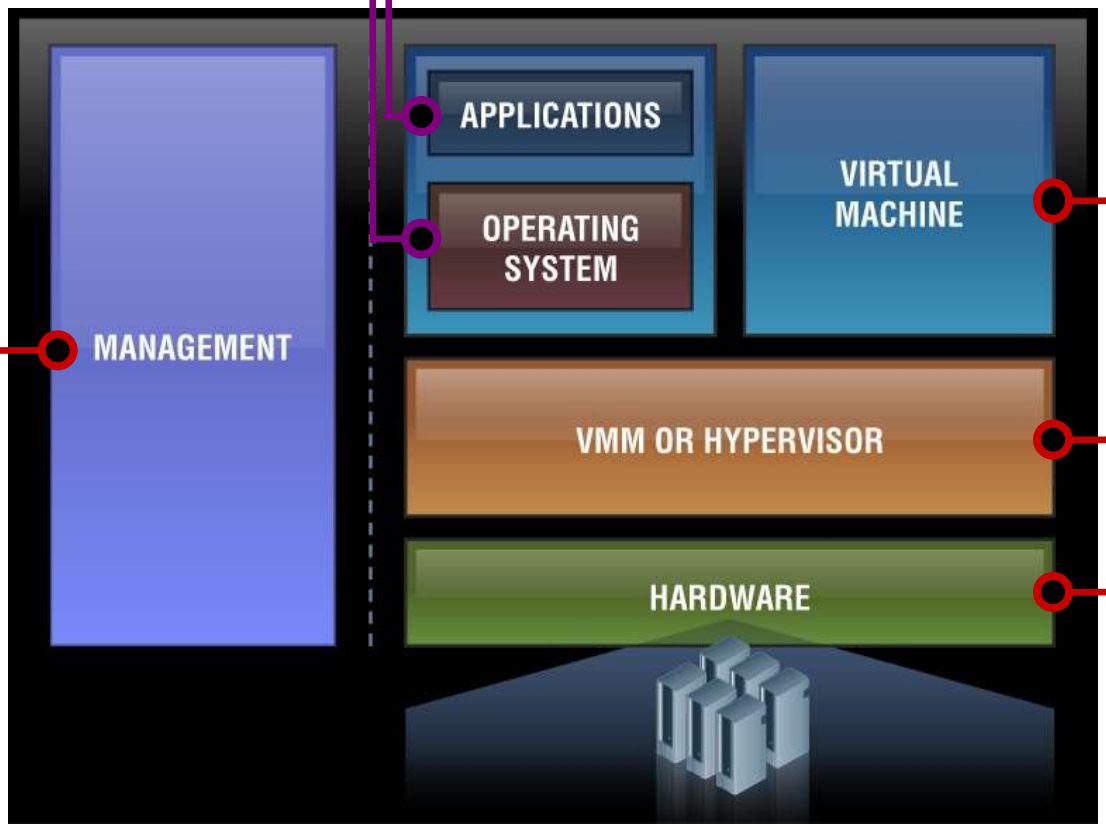
- Все
  - Динамический гибкий ЦОД
  - Пул ресурсов
  - Стандартизация
  - Повышение эффективности
- Ничего
  - Виртуальные ИТ – это все равно ИТ

    Безопасность, управление, сложность, гетерогенность
- Виртуализация != Безопасность
  - ВМ не более безопасны, чем стандартные сервера
- Применимы те же принципы безопасности
  - Многоуровневая защита
  - Сегментация сети
  - Централизованное управление безопасностью

Больше компонент = больше рисков

- Традиционные угрозы
- Новые угрозы виртуальных сред

ОС и приложения можно атаковать, как и раньше



Компрометация уровня управления

Хранение ВМ и данных управления

Требуются новые навыки

Появление “чужих” ВМ

Динамическое перемещение

Кража ВМ

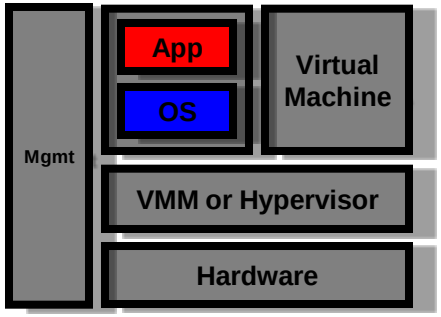
Изменение квот ресурсов

Единая точка отказа

Руткиты в hardware

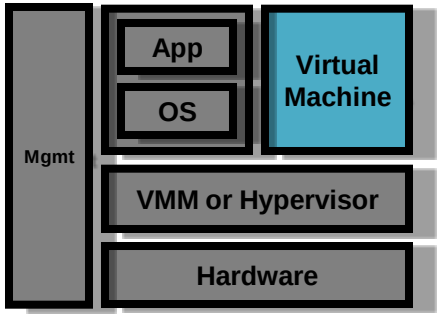
Виртуальные NICs & виртуальное hardware – цели

Операционные системы и приложения



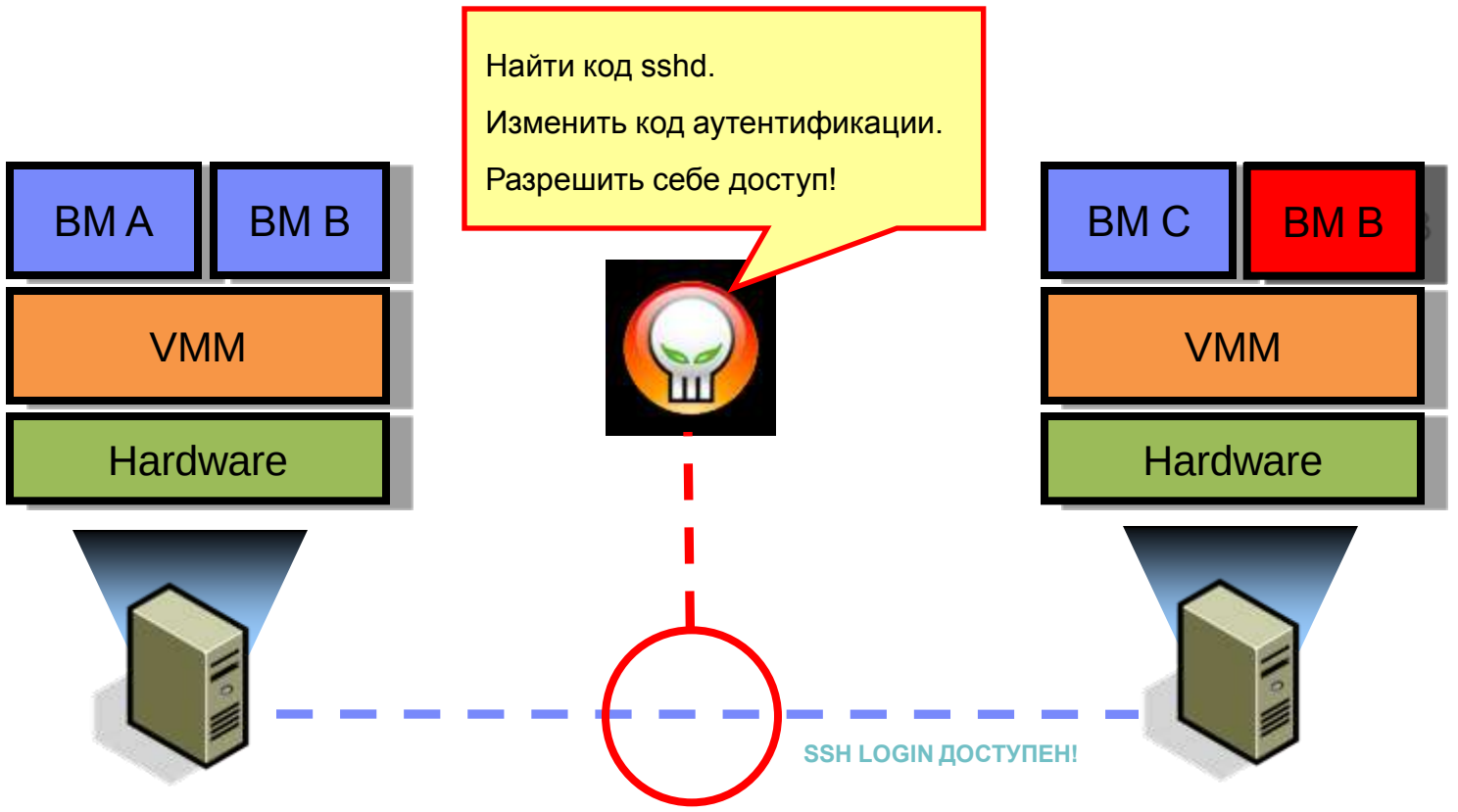
- Традиционные угрозы сохраняются
  - Вредоносное ПО: вирусы, черви, трояны, руткиты
  - DoS и DDoS-атаки
  - Переполнения буфера, инъекции SQL, XSS
  - Утечки конфиденциальных данных
- Отказо- и катастрофоустойчивость, которую обеспечивает виртуализация, не повышает “врожденную” сопротивляемость ОС и приложений к атакам

Виртуальные машины



- Установка патчей
  - Возможность останавливать/восстанавливать ВМ “мешает” установке патчей
- Неконтролируемое появление ВМ
  - Нелегко отслеживать, появление неуправляемых ВМ, “чужих” ВМ
- Динамическое перемещение (Live Migration, VMotion)
  - А если ВМ перемещается на менее защищенный физический центр, сеть, ЦОД?

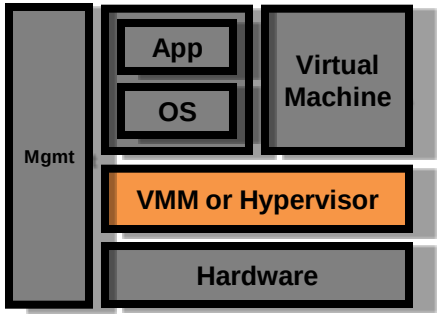
Атака на Live Migration: Xensploit



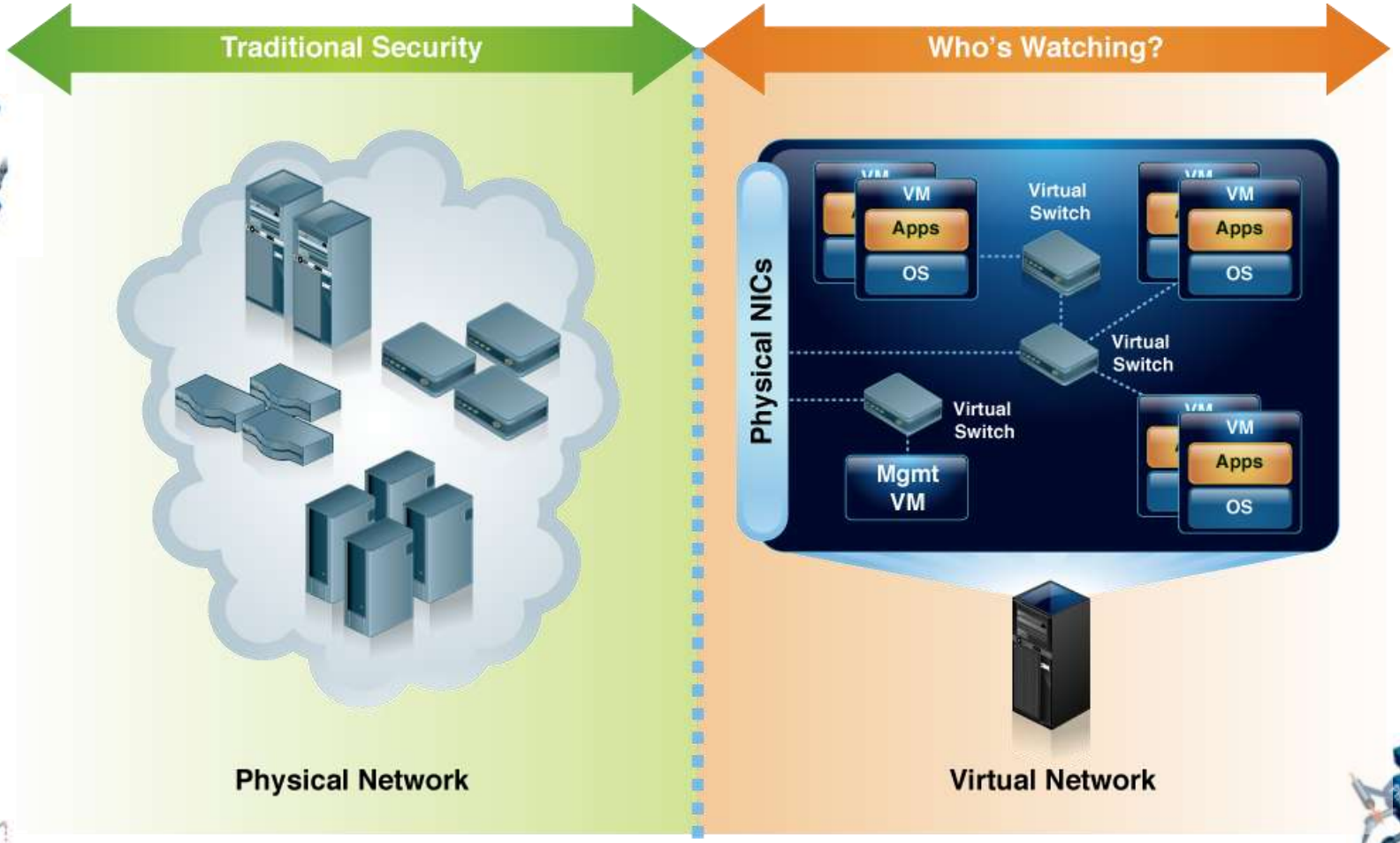
По умолчанию, трафик live migration пересылается по сети в открытом виде. Атака «человек посредине» может использоваться для захвата управления ВМ.

VMM или гипервизор

- Новые уязвимости – новые вектора атак
- Единая точка отказа
- Неавторизованное изменение квот ресурсов
- Анализ трафика между ВМ - «мертвая зона»

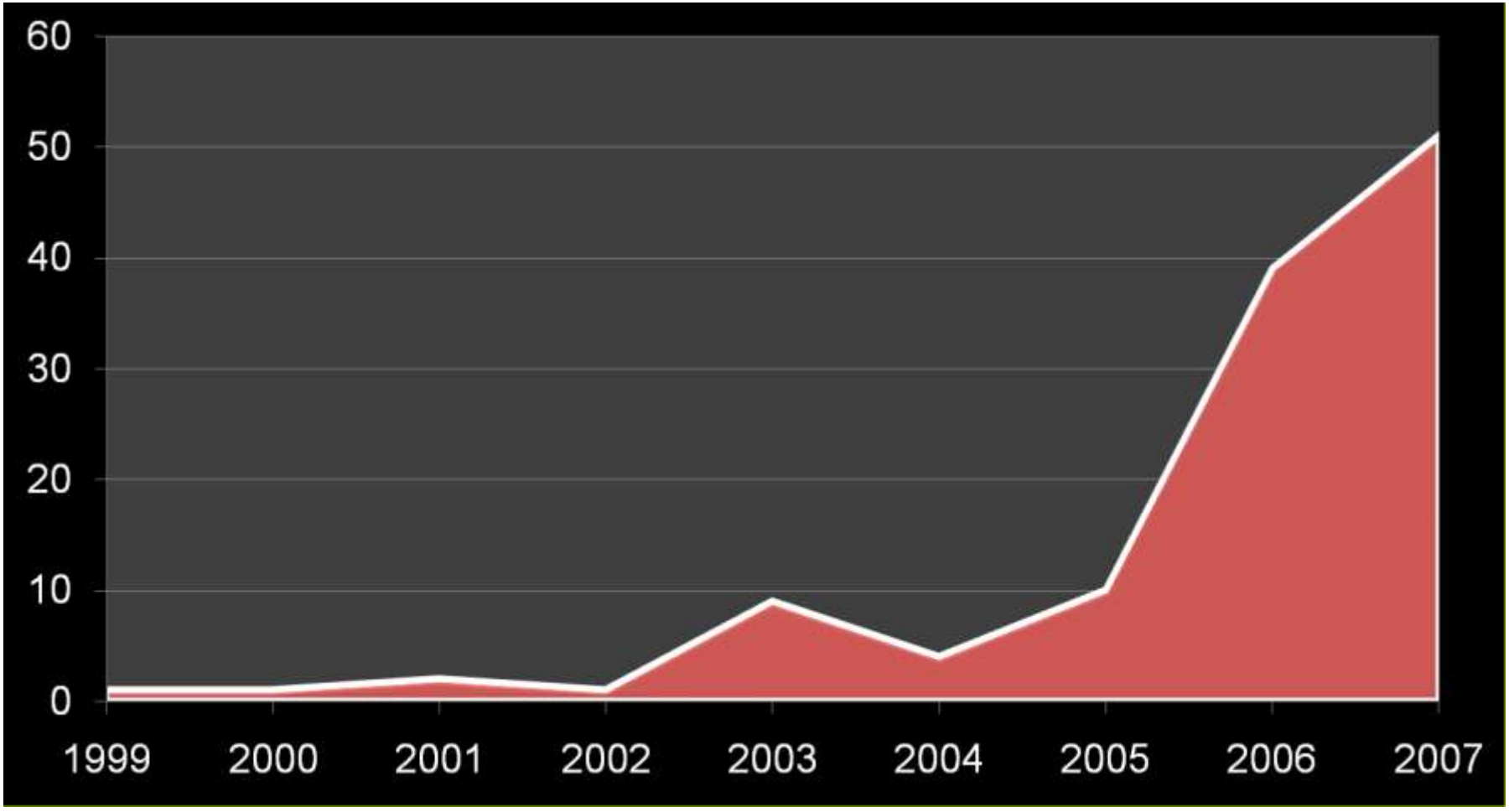


Конвергенция сервера и сети

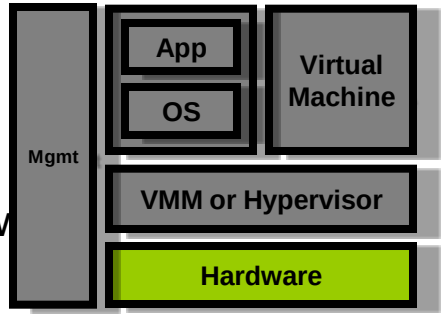


Уязвимости в ПО виртуализации

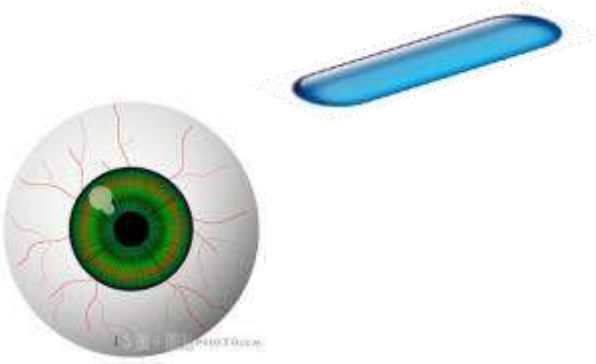
По данным IBM X-Force: VMware, Xen, Virtual PC, QEMU, Parallels и т.д.



Виртуализированная аппаратная часть



- Встроенная поддержка виртуализации (Intel-VT, AMD-V)
  - Стелс-технологии – руткиты в виртуализированном hardw
  - Низкоуровневый код – сложнее обнаружить
  - Blue Pill – руткит, вредоносный гипервизор для AMD-V
  - Vitriol – то же для Intel-VT



План

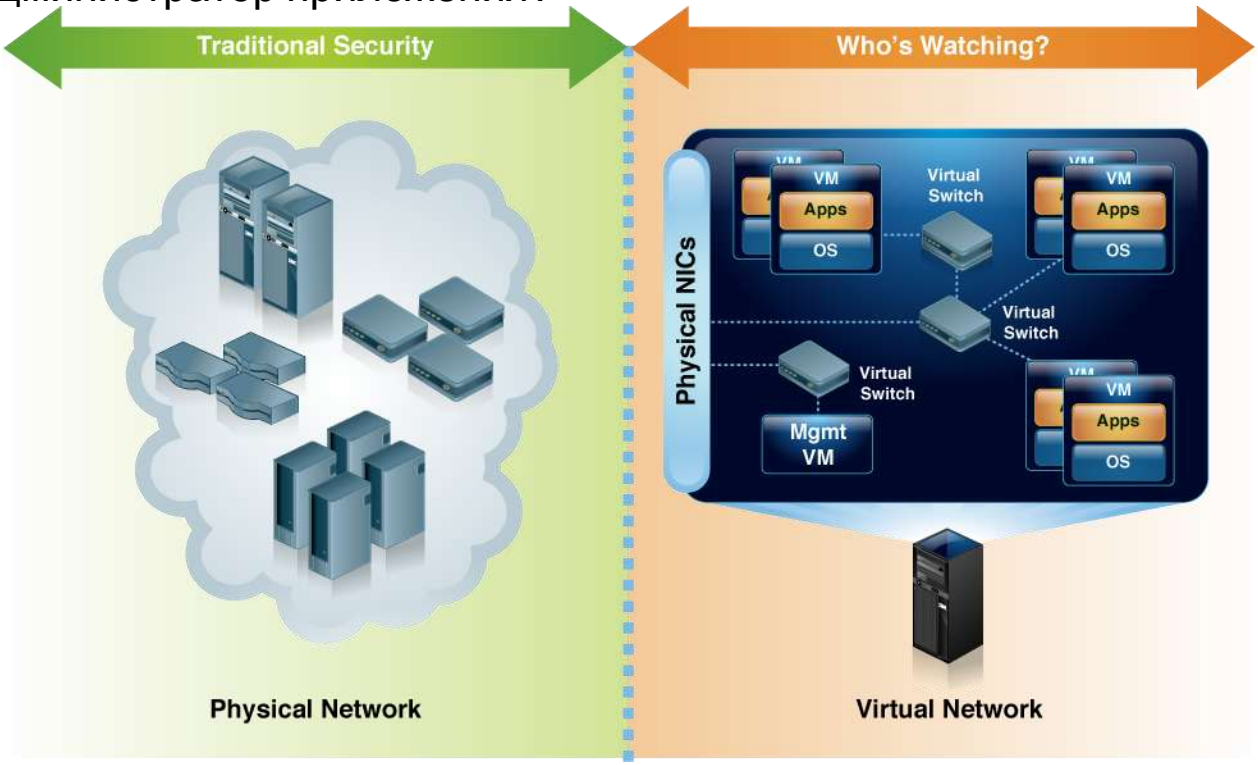
Виртуализация — новые технические риски

Виртуализация — новые организационные риски

Защита виртуальной инфраструктуры — IBM Security Virtual Server Protection

Кто владелец?

- Сетевой администратор?
- Администратор сервера? Какого?
- Администратор СУБД?
- Владелец/администратор приложения?



Кто владелец?

- “Захват земли”
- “Горячая картошка”
- “Это ты виноват!”

Операционные трудности

- Live Migration – необходимо отслеживать местонахождение ВМ
- Управление патчами/конфигурацией
  - Pause/Offline/Suspend/Activate влияют на:
    - Сканирование уязвимостей
    - Установку патчей
- Управление образами ВМ
  - Защищенное хранение
  - Управление версиями

Определите политики и регламенты

- Пока это все не вышло из-под контроля:
  - Роли и зоны ответственности администраторов
  - Политику выделения ресурсов
  - Управление образами ВМ
  - Требования безопасности

План

Виртуализация — новые технические риски

Виртуализация — новые организационные риски

Защита виртуальной инфраструктуры — IBM Security Virtual Server Protection

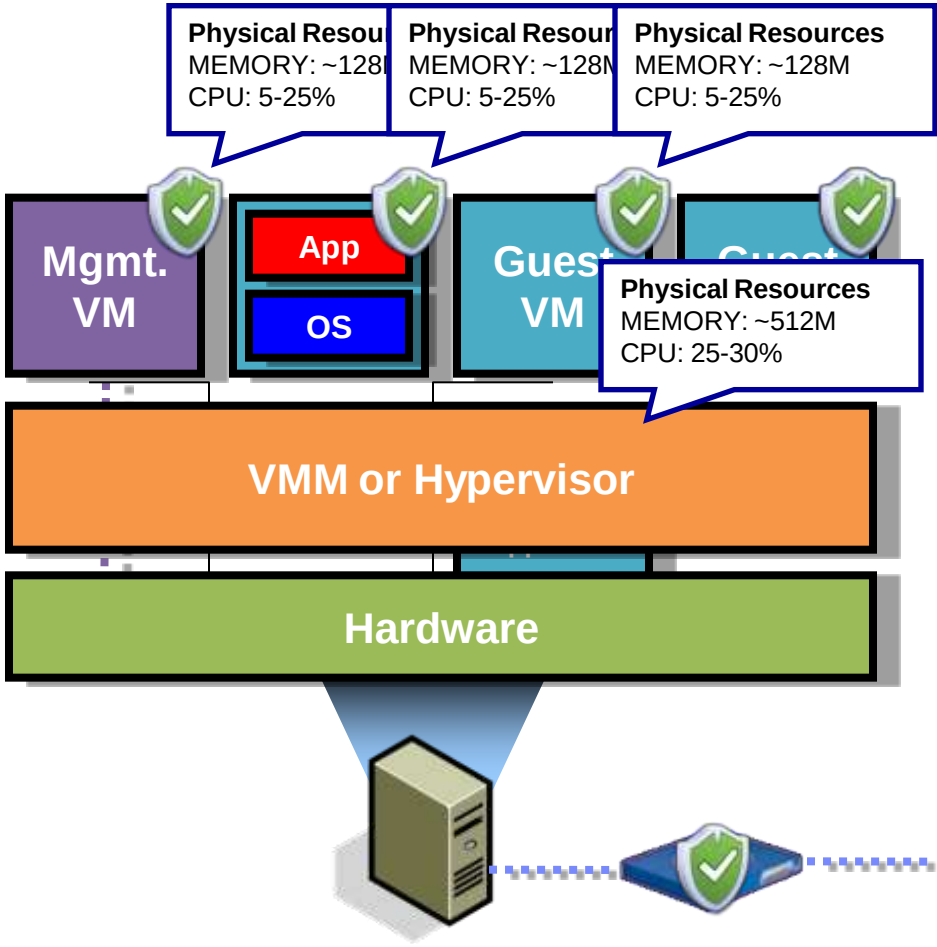
Защита виртуализации традиционными средствами

- Агент безопасности в каждой ВМ
- Дополнительные уровни защиты
- Сегментирование сети на VLANы
- Виртуальные устройства защиты

Потенциальные сложности и ограничения:

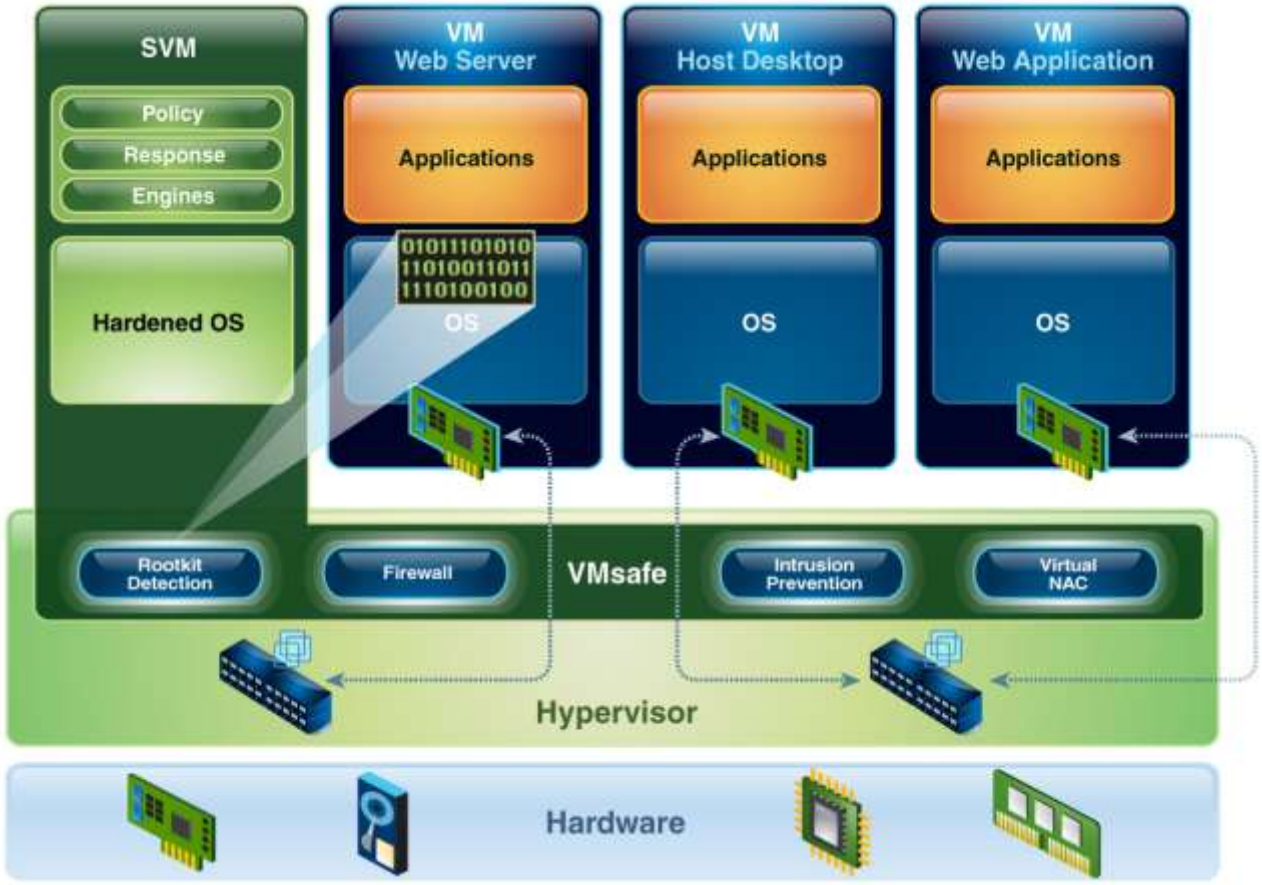
- В новые ВМ надо ставить агента
- Гетерогенная среда – разные агенты
- Избыток безопасности = затраты ресурсов
- Кошмар управления
- Доверие VMM

Нужно интегрировать безопасность прямо в виртуальную инфраструктуру!



IBM Security Virtual Server Protection

Предоставляет всеобъемлющую, интегрированную защиту виртуальной инфраструктуры в *одном продукте*



- Межсетевой экран
- Интеграция с VMsafe
- Обнаружение руткитов
- Обнаружение и предотвращение вторжений
- Анализ трафика между ВМ
- Управление разрастанием ВМ
- Принудительные политики использования сети
- Автоматическая защита для VMotion
- Автоматическое обнаружение новых ВМ
- Аудит виртуальной инфраструктуры (Доступ привилегированных пользователей)
- Защита виртуальных сегментов сети
- Virtual Network Access Control
- Централизованное управление
- Защита Web-приложений
- Виртуальный патч

IBM Security VSP — интегрированные преимущества

- Прозрачность
  - Без реконфигурации виртуальной сети
  - Без изменений гостевых ОС
- Консолидация безопасности
  - Одна Security Virtual Machine (SVM) на физический сервер
  - Отношение защита:ВМ — 1:много
- Автоматизация
  - Обнаружение новых ВМ
  - Применение к ним политик безопасности
- Эффективность
  - Исключение повторяющихся задач
  - Распределение нагрузки на уровне сети
- Защита любой гостевой ОС

IBM Security VSP — интегрированные преимущества

- Динамическая безопасность где бы ни находилась ВМ
- Протоколо-независимый анализ и защита, основанная на уязвимостях
- Виртуальный Патч — защита независимо от стратегии установки патчей на ВМ
- Контроль доступа к виртуальной сети, ограничение доступа до применения политик безопасности
- Аудит привилегированного доступа к виртуальной инфраструктуре
- Защита ядра гостевых ОС, обнаружение руткитов

> “IBM представил первую коммерческую реализацию обнаружения/предотвращения руткитов, работающую вне среды защищаемых виртуальных машин...”
>
> -Нил Макдональд, Gartner

Спасибо!

Для дополнительной информации:
ibm.com/security

Или:
Oleg.Letaev@ru.ibm.com