Защита критически важных данных от кибератак

Юрий Латышевский

Dell EMC

GLOBAL SPONSORS

УРОК КОТОРЫЙ МЫ ПРОШЛИ И СДЕЛАЛИ ВЫВОДЫ

Текущий климат безопасности

Эволюция киберугроз

Традиционные угрозы

- Кибер воры
- Кибер атаки
  - Отказ в сервисе

Новые угрозы

- Кибер уничтожение
  - Основных и резервных копий
  - Хактивизм
- Кибер вымогательство
  - Ransomware
    - Более продвинуто
    - Более деструктивное
    - Более дорогостоящее

Рекомендации регуляторов

— NIST CSF

National Security Agency: “лучшие практики защитить информационные системы и сети от деструктивной атаки злоумышленников включает… ***Изоляцию сетевых систем***”

Securities and Exchange Commission: Серия ***последних событий*** включает ситуации с дальнейшим освещением необходимости участников рынка зарезервировать операционную целостность своих автоматизированных систем.”

Federal Reserve System: “Финансовые институции должны рассмотреть к применению следующие шаги… Такие как логическую сегментацию сети, жёсткое резервное копирование, воздушный зазор и физическую сегментацию критических систем”

European Banking Authority: “Компетентные органы должны знать, имеет ли организация ***всеобъемлющий протестированный план обеспечения отказоустойчивости и восстановления после аварии***”

Federal Financial Institutions Examination Council (FFIEC): “***архитектуры резервного копирования с воздушным зазором*** лимитируют возможности применения кибератак и позволяют восстановить данные на точку перед атакой.”

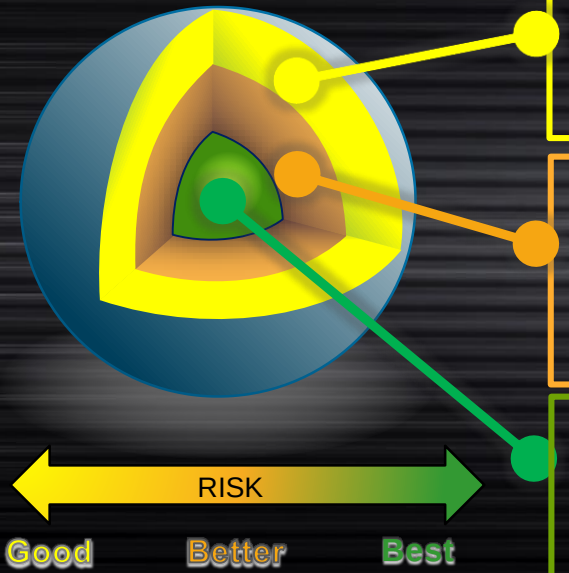
“**National Association of Insurance Commissioners:** “.. Жизненной необходимостью государственных регуляторов предоставить ***эффективный гид безопасности по защите*** данных и инфраструктуры..”

FFIEC
FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL

EBA European Banking Authority

NAIC
National Association of Insurance Commissioners

Многоуровневая безопасность защиты данных



Традиционная защита данных: Лучшие практики

- Развёртывание многослойной защиты данных для наиболее критических систем всегда включает восстановление на точку времени и независимые резервные копии с репликацией на резервную площадку (N+1)

Дополнительные закрепляющие функции

- специфические инструкции сервиса резервного копирования и восстановления
- Шифрование на лету и в пост процессе
- Блокировки на удаление с доступом отдельного офицера по безопасности

Продвинутые сервисы защиты

- Решение изолированного восстановления
- Сервисы (доступ, план, внедрение, и проверка)
- Использование аналитику безопасности
  - RSA Security Analytics

Для чего нужна резервная копия

согласно IDC:

“Копия данных создаётся копированием первичных данных с целью защитить данные и операции, аналитики, разработки.”

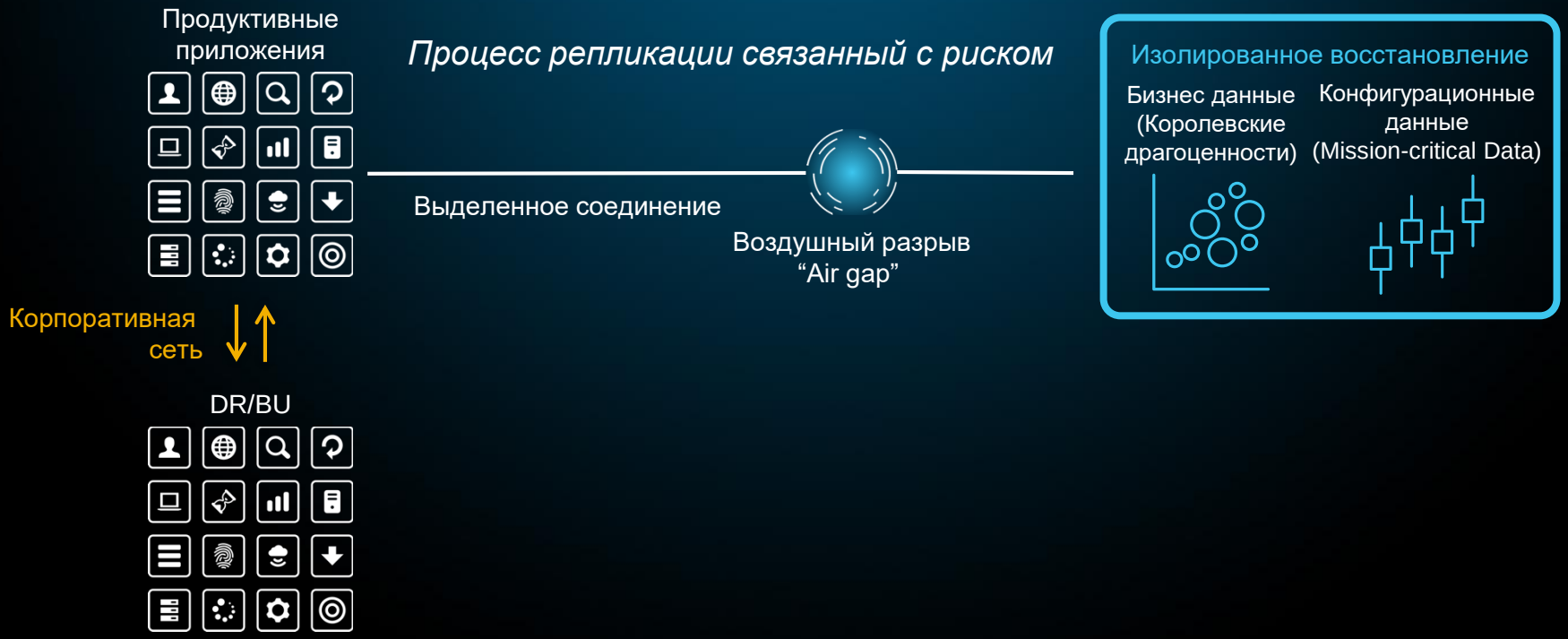
Угроза порчи данных может исходить как извне так и изнутри организации

Не обязательно обслуживающему персоналу знать что все действия копируются

Защита конечных точек и данных в облаке

Изолированное восстановление – как оно работает?

Критичные данные находятся за пределы сетки и изолированы

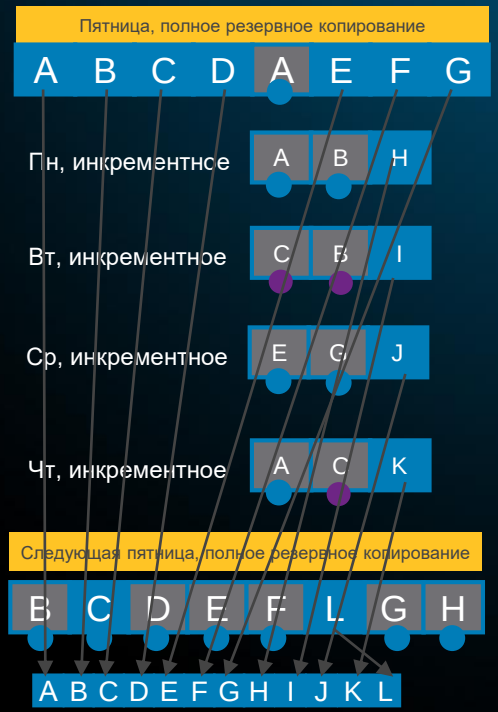


Изолированное восстановление – Data Domain

- Создание резервной копии
- Включение соединения и репликация на изолированную систему
- Завершение репликации и выключение соединения
- Система изолирована
- Включение соединения и восстановление

Дедупликация – Data Domain

- Хранение большего объема резервных копий на меньшей площади



ПЯТНИЦА, ПОЛНОЕ	1 ТБ	В 2—4 раза	250 ГБ
Понедельник, инкрементное	50 ГБ	В 7—10 раз	5 ГБ
Вторник, инкрементное	50 ГБ	В 7—10 раз	5 ГБ
Среда, инкрементное	50 ГБ	В 7—10 раз	5 ГБ
Четверг, инкрементное	50 ГБ	В 7—10 раз	5 ГБ
Следующая ПЯТНИЦА, ПОЛНОЕ	1 ТБ	В 50—60 раз	18 ГБ
ИТОГО	2,2 ТБ	В 7,6 раза	288 ГБ

Надёжность хранения – Data Domain

Сквозная проверка данных
- Контрольная сумма
- Дедупликация, запись на диск
- Проверка

Самовосстановление файловой системы
- Очистка
- Устаревшие данные
- Дефрагментация
- Проверка

Другое
- RAID 6
- NVRAM
- Снимки

Защита данных – Data Domain

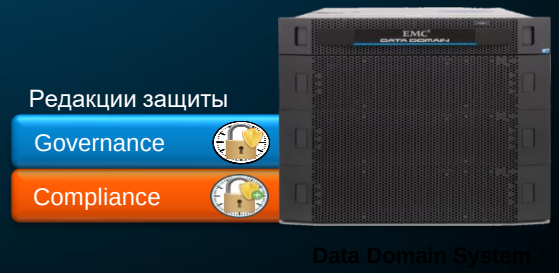
СТРАТЕГИЧЕСКОЕ УПРАВЛЕНИЕ И СООТВЕТСТВИЕ АРХИВНЫХ ДАННЫХ ТРЕБОВАНИЯМ РЕГУЛЯТОРОВ SEC 17a-4(f)

NIST National Institute of Standards and Technology U.S. Department of Commerce

Protect

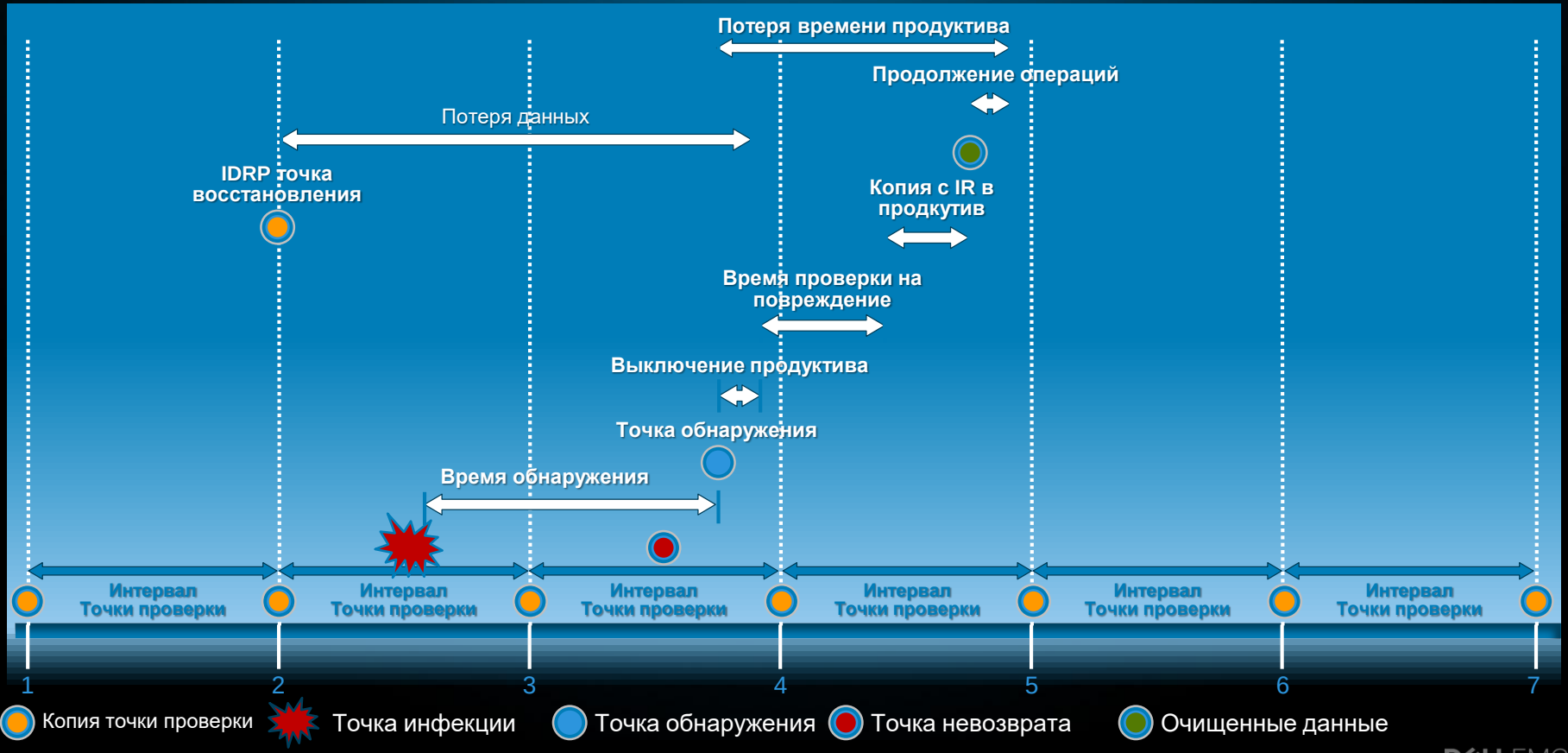
Recover

- Не позволяет модифицировать или удалить данные резервных копий
- Резервные копии не могут быть изменены, повреждены или удалены – даже с административным доступом
- Двойная авторизация обеспечивает административные работы под контролем выше чем администратор
- Дополнительная защита против Ransomware, порчи и других деструктивных атак

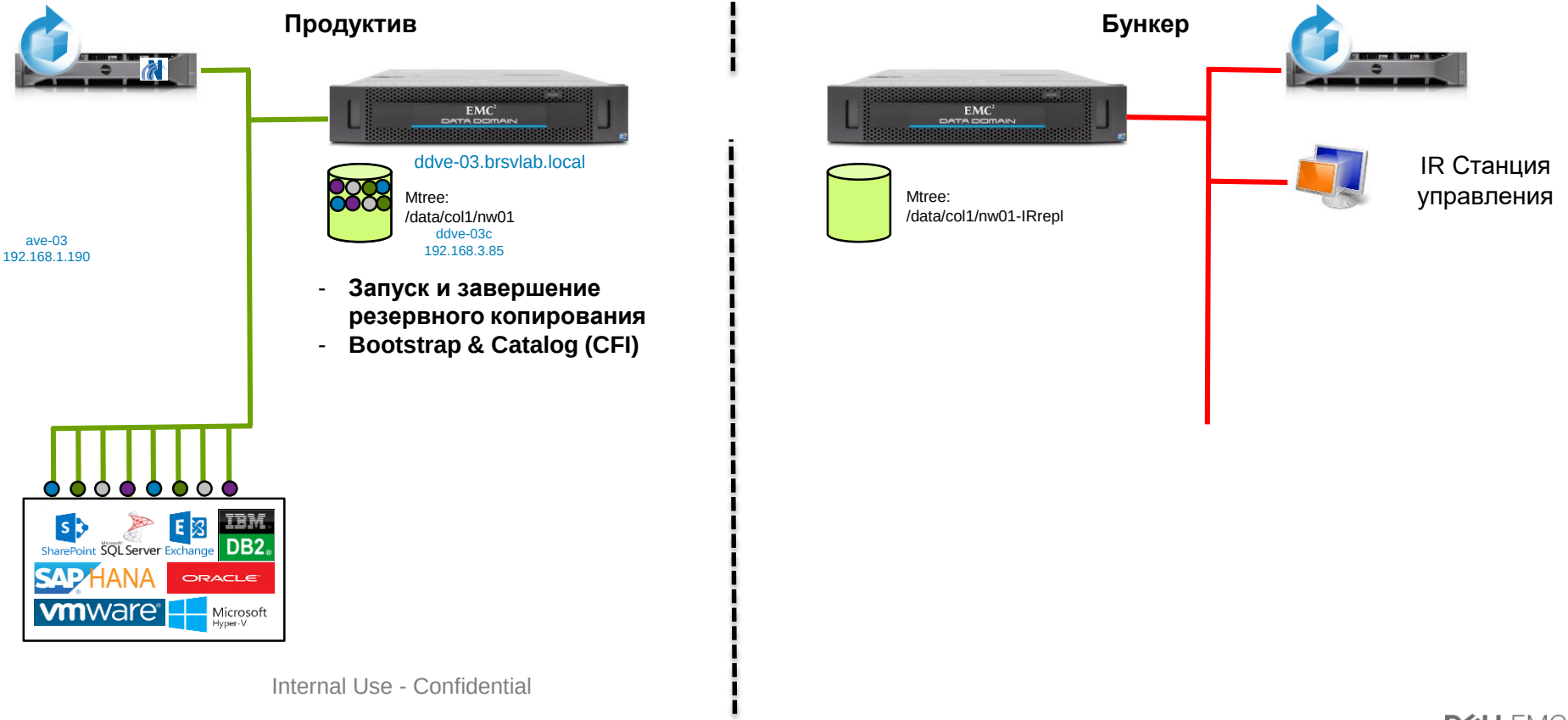


DELL EMC

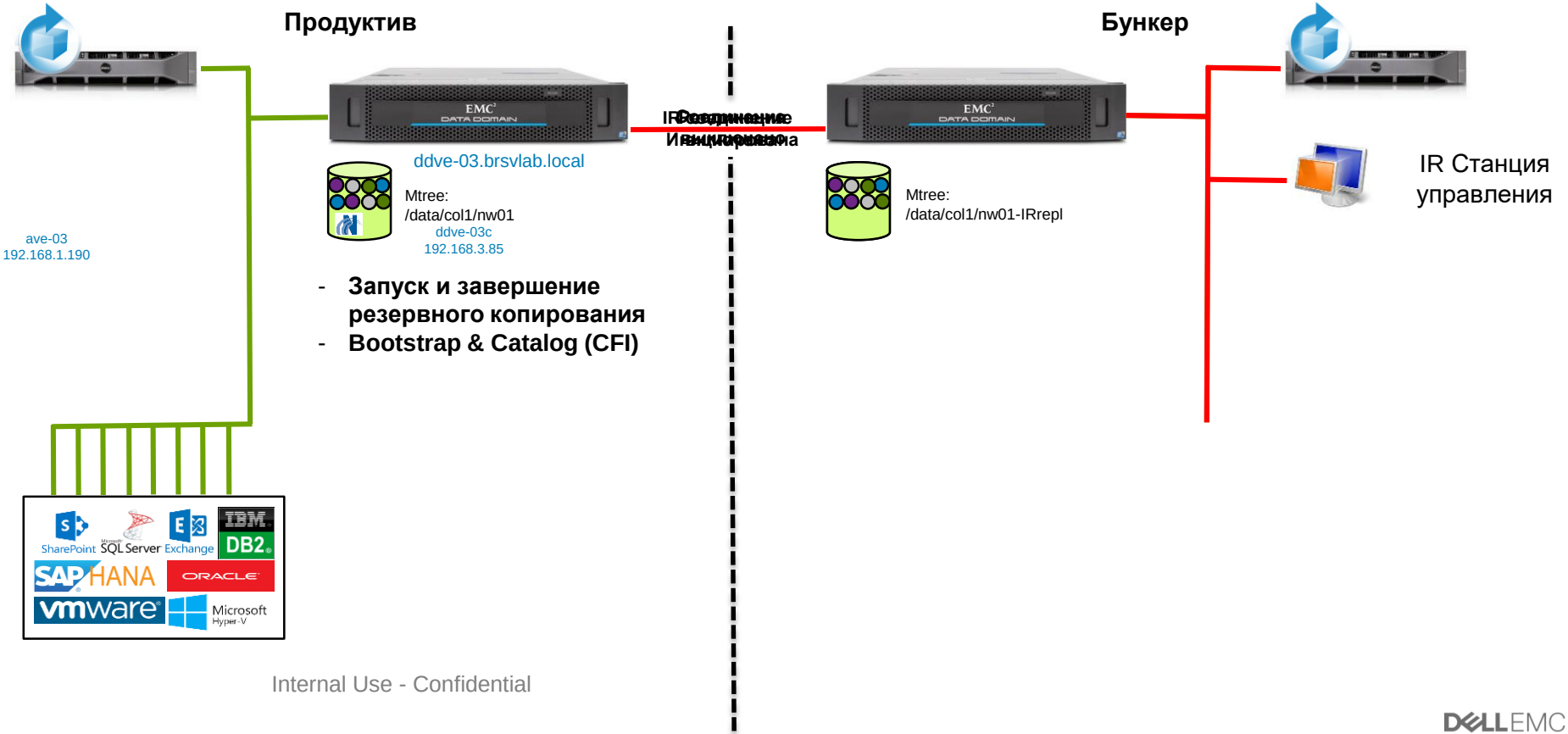
IR – Восстановление с копии точки проверки



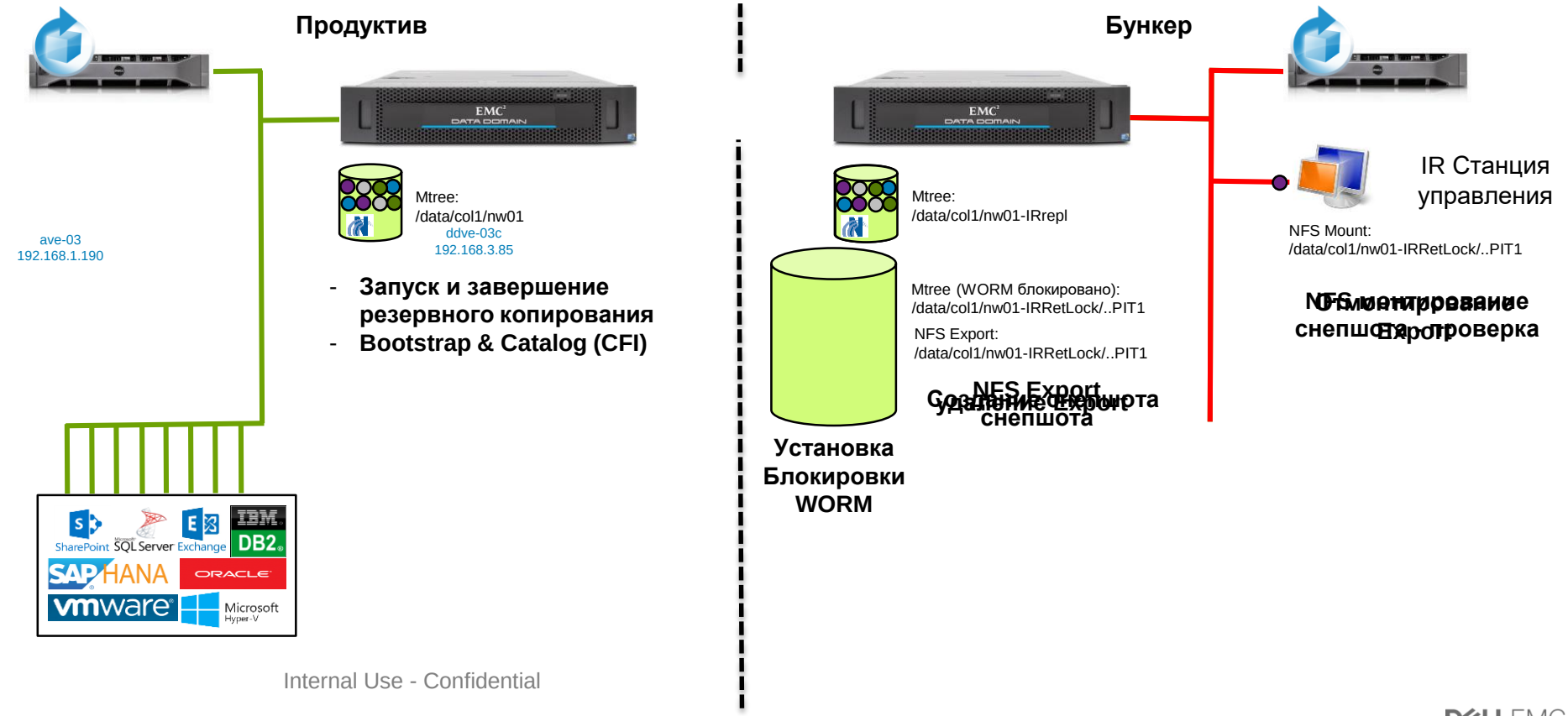
Изолированное восстановление- Networker



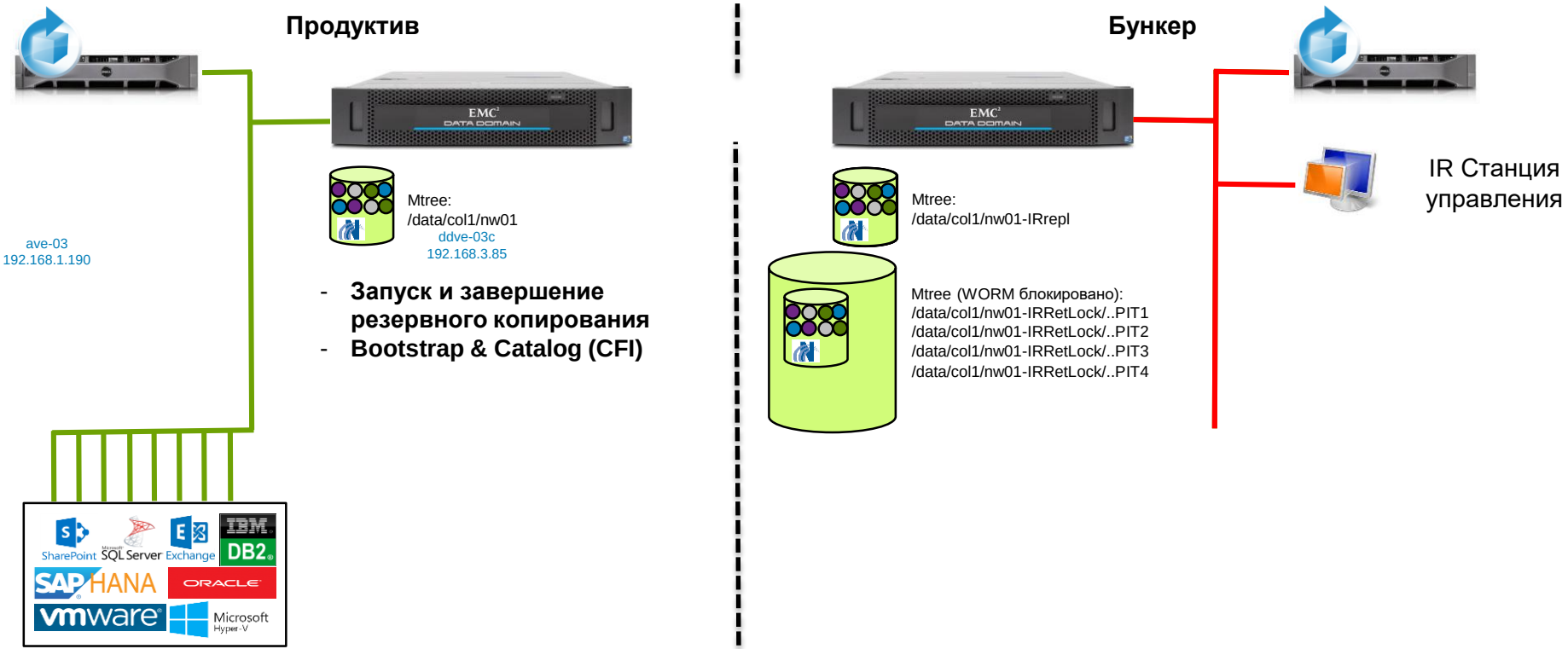
Изолированное восстановление- Networker



Изолированное восстановление- Networker



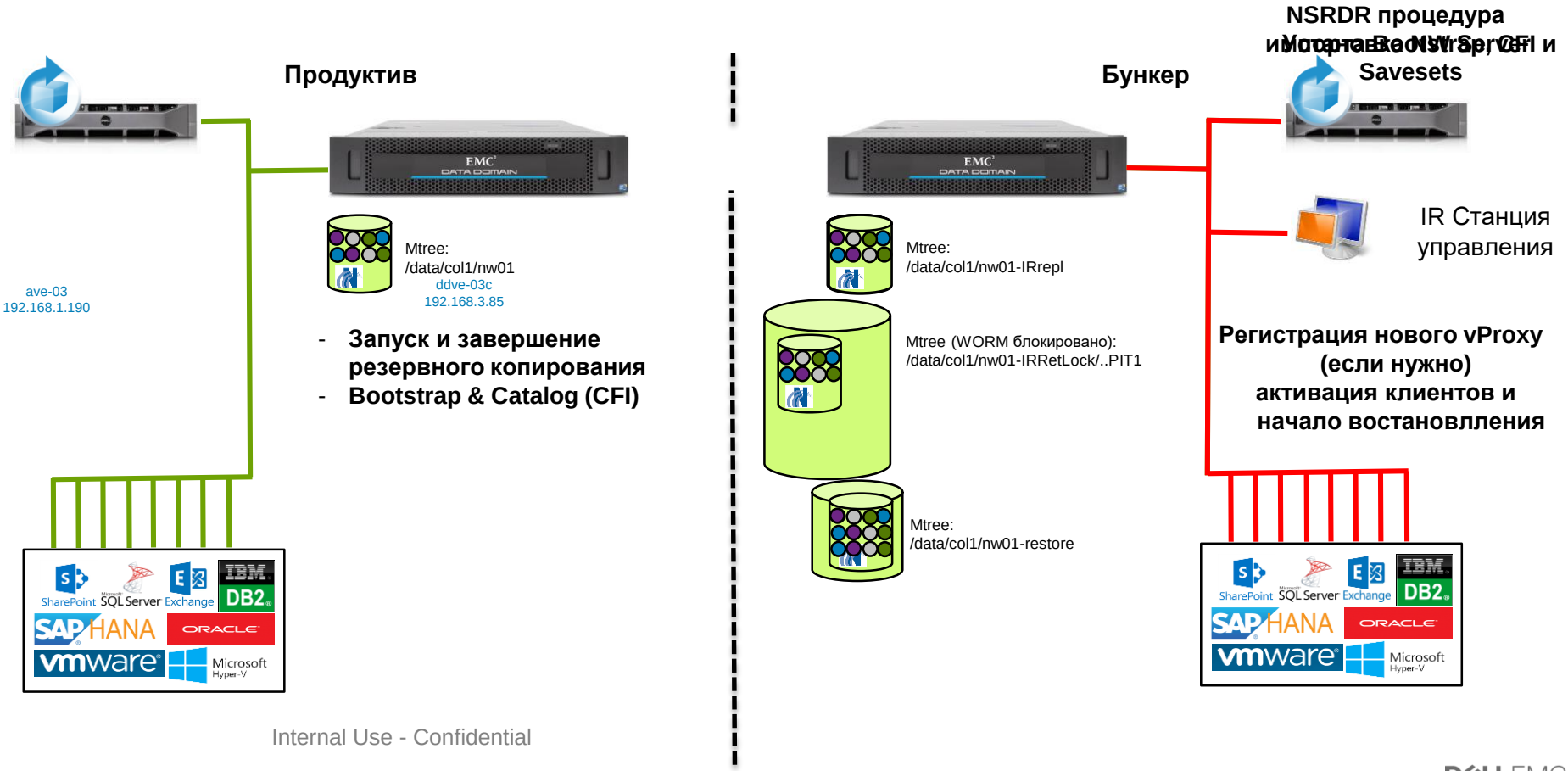
Изолированное восстановление- Networker



- **Запуск и завершение резервного копирования**
- **Bootstrap & Catalog (CFI)**

Изолированное восстановление- Networker

Изолированное восстановление- Networker



IR (изолированное восстановление) дополняет DR (восстановление после аварии)

Системы изолированы

Среды отключены от сети и пользователей кроме тех кто проверенные

Периодичное копирование данных

Программа автоматизирует копирование данных на вторичное хранилище

Проверка целостности и сигнализация

Восстановление и выздоровление

Процедуры(т.к., Run Books) для восстановления / и выздоровления после инцидента


DELL EMC