

Как финансовой организации заработать деньги там, где большинство их теряет

Ильдар Суханов

Технический консультант по инфраструктурным решениям

DELLTechnologies



INCREASE

YOUR AGILITY & FLEXIBILITY

Готовы ли вы к тому, что будет дальше?

Как ИТ-организация отреагирует в следующий раз, когда бизнес обратится к ним?

Можете ли вы обеспечить маневренность и гибкость, которые потребуются вашей организации?

Наш мир ускорился

И ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ДОЛЖНА БЫТЬ УСКОРЕНА С НИМ



1. Dell Technologies Digital Transformation Index, October 2020. Research conducted by Vanson Bourne surveying 4,300 business leaders across 18 countries. <https://www.delltechnologies.com/dtindex>
2. IDC FutureScape Highlights What Will Happen Next as Enterprises and the IT Industry Respond to the Disruptions Caused by COVID-19. 27 Oct 2020
3. Gartner, "How to Use Consumption-Based Procurement Models for On-Premises Infrastructure." Published 20 September 2019

Изменение мышления

сперва
ИНФРАСТРУКТУРА

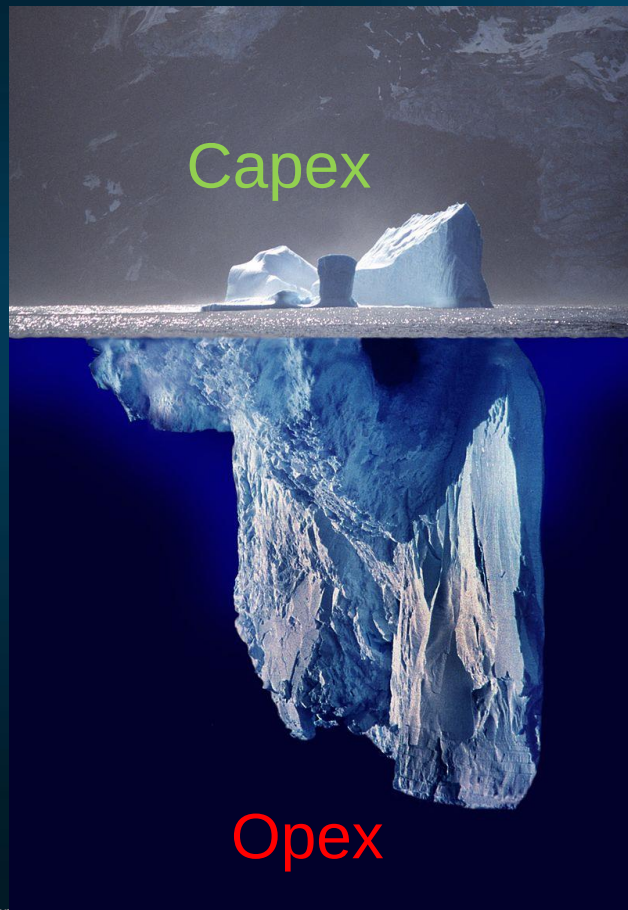


сперва
ДАННЫЕ



Ваш самый ценный актив хранится в нужном месте, в нужное время и с правильным соглашением об уровне обслуживания

Айсберг — новый взгляд на ваши ИТ



- Начальная цена покупки
 - Расходы, связанные с закупками
- 20..40%?

- ✓ Стоимость миграции
 - ✓ Тренинги для ИТ
 - ✓ Время простоя
 - ✓ Расходы на ИТ-администрирование
 - ✓ Стоимость технического обслуживания
 - ✓ Стоимость места
 - ✓ Затраты на охлаждение
 - ✓ Затраты на электроэнергию
 - ✓ Затраты на будущую совместимость
 - ✓ Инфляция
 - ✓ Новое законодательство
- 60..80%?

Что вам нужно в вашем оборудовании?

Производительность, требования, цена

Примеры подхода

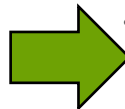
Полезная емкость

- Определение из 1990-х — ориентировано на жесткие диски
- Сжатие и дедупликация не учитываются
- Предпочитается ИТ-специалистами

Эффективная емкость

- Определение появилось на AFA только в 2014..2017 гг.
- Максимизация рентабельности инвестиций (ROI) при снижении эксплуатационных расходов (сжатие и дедупликация)
- Используется бизнесом

100 ТБайт



25 ТБайт

Охлаждение, Потребляемая мощность, размер, стоимость обслуживания, цена

Синхронная репликация

- Определение конца 1990-х
- Может потребоваться одно и то же оборудование на обоих ЦОД
- Может серьезно повлиять на производительность в случае сбоя или простоя
- Предпочитается ИТ-специалистами

Метро/Растянутый кластер

- Определение появилось примерно в 2010 году.
- Нет простоев, нет влияния на производительность
- Может работать между оборудованием разных поставщиков
- Используется бизнесом

~120 секунд



0 секунд

Нет гарантированных простоев, нет влияния на бизнес

DELL Technologies

3 идеи цифровой трансформации

Agility



HCI как новая платформа
(VxRail & PowerFlex)

Надежность



Банковские сервисы
доступны всегда
и в любое время
(Metro-конфигурация)

Безопасность



Cyber Resiliency
Данные защищены
всегда и против
неизвестных угроз

Повышение эффективности | Снижение OpEx

Преимущества внедрения HSI

Agility



Скорость публичного облака, эффективность и экономичность в центре обработки данных

Масштабируемость



Начните с малого и легко увеличивайте масштаб, сохраняя при этом уровень производительности.

Простота



Упрощение операций с помощью программной автоматизации и управления жизненным циклом

Повышение эффективности | Снижение OpEx

HCI против Классической архитектуры

90%

Низкие административные расходы

82%

Сокращение времени развертывания

50%

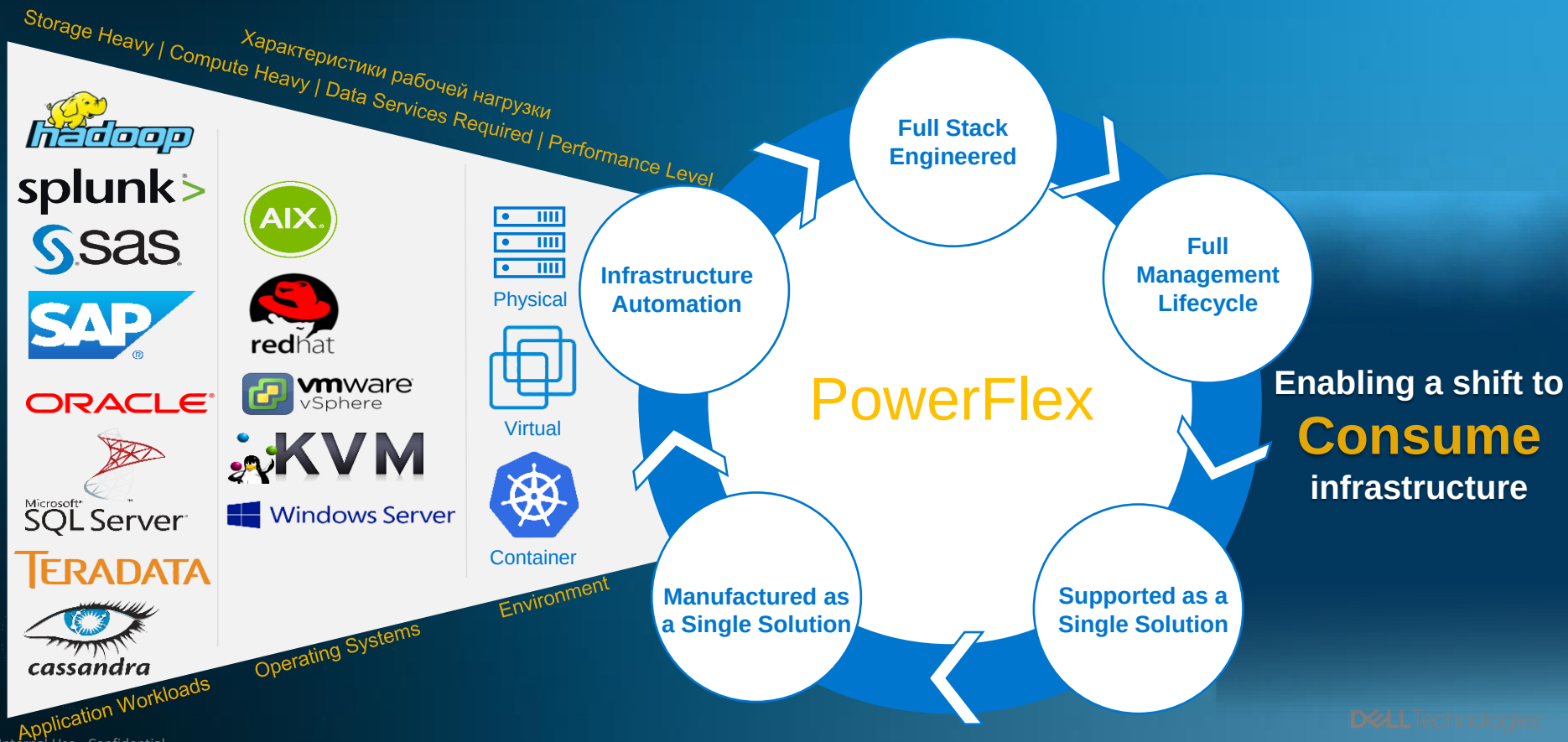
Меньше стоимость первоначальной покупки



Несколько гипервизоров
или Bare metal

Высокопроизводительные
базы данных и приложения

PowerFlex как общая платформа центра обработки данных



Что мы подразумеваем под RTO, RPO и DTO?



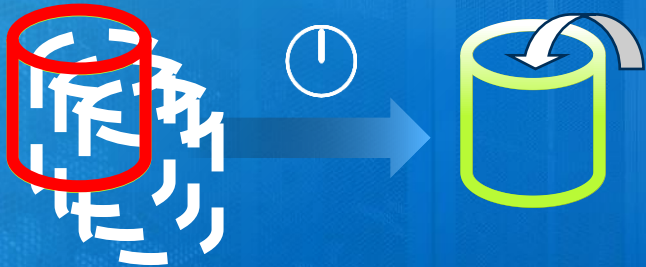
RTO (Recovery Time Objective) – Целевое время восстановления
Сколько времени требуется для восстановления?

RPO (Recovery point objective) – Целевая точка восстановления
Сколько данных потеряется?



DTO (Decision Time Objective) — целевое время принятия решения
Сколько времени необходимо для принятия решения об отработке отказа?

Каковы различные режимы репликации?



- Асинхронный — данные отправляются периодически
- $RPO > 0$
- $RTO > 0$
- $DTO > 0$

- Синхронный — обе системы полностью зеркальны
- $RPO = 0$
- $RTO > 0$
- $DTO > 0$



- Metro — обе системы зеркальны, И данные полностью доступны на обоих сайтах
- $RPO = 0$
- $RTO = 0$
- $DTO = 0$

Только Metro-репликация дает настоящие $RTO=0$ и $RPO=0$
Большинство приложений допускают простои только в течение 30 секунд!

Известные атаки программ-вымогателей

11 Ransomware Hit ATM Giant Diebold Nixdorf

MAY 20

Diebold Nixdorf, a major provider of automatic teller machines (ATMs) and payment
te disrupted
S customer
m

Garmin reportedly paid multimillion-dollar ransom after suffering cyberattack

A reported \$10 million was demanded in ransom
took Garmin services offline

Canon confirms major ransomware attack has taken down its systems

Colonial Pipeline Paid Roughly \$5 Million in Ransom to Hackers

The payment clears the way for gas to begin flowing and
risks emboldening other criminal groups to take American
companies hostage by seizing control of their computer

200 businesses hit by ransomware after breach at Florida IT firm

PUBLISHED FRI, JUL 2 2021 6:27 PM EDT

REUTERS

SHARE [f](#) [t](#) [in](#) [✉](#)

KEY POINTS

- Cybersecurity company Huntress Labs said on Friday that 200 businesses have been hit by ransomware attacks following an incident at U.S. IT firm Kaseya in Miami.

Аварийное восстановление не является кибервосстановлением

Аварийное восстановление / непрерывность бизнеса недостаточны для борьбы с современными киберугрозами

Категория	Аварийное восстановление	Киберустойчивость
Время восстановления	Близко к мгновенному	Надежно и быстро
Точка восстановления	Идеально непрерывная	в среднем за 1 день
Природа катастрофы	наводнение, отключение электроэнергии, погода	Целевая Кибератака
Последствия стихийного бедствия	региональный;	Глобальный; быстро распространяется
Топология	несколько целей	Изолировано, в дополнение к DR
Объем данных	Комплексный, все данные	Выборочный, включает базовые услуги
Восстановление	Стандартное аварийное восстановление (например, переключение на другой сайт)	Интерактивное выборочное восстановление; часть CR

Непрерывность бизнеса

Резервное копирование :

- 100% всех данных
- Локальные → Внешние → Архив
- Более высокие точки восстановления
- Более длительное время восстановления
- Проверка

Аварийное восстановление:

- 60-90% всех данных
- В зависимости приложений
- Уровень приложений
- Репликация
 - Более низкая целевая точка восстановления (RPO)
- Тестирование
 - Более низкое целевое время восстановления (RTO)

Киберустойчивость:

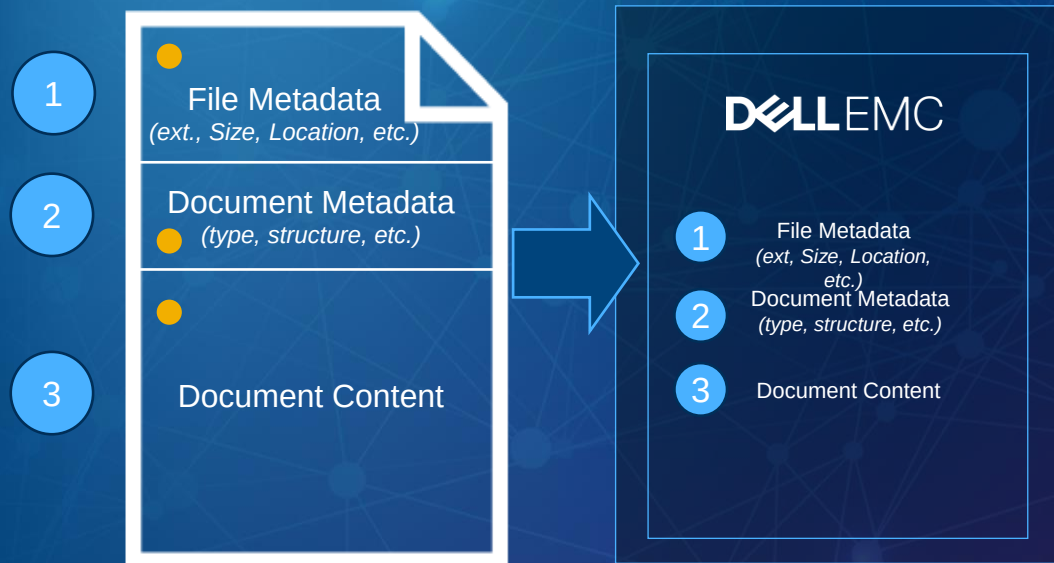
- 15-30% всех данных
- Физически отдельная среда
- Физически безопасная среда
- Логический «воздушный зазор»
- Неизменяемая копия
 - Блокировка изменений
- Более короткое хранение
 - 14-35 дней
- Проактивная аналитика и отчетность
 - Cybersense: обнаружение компрометации и предоставление криминалистической экспертизы
- Ответ на уровне аварийного восстановления
- Валидация + Тестирование

Как работает CyberSense

Возможности аналитики

Анатомия файла

Локальный механизм аналитики



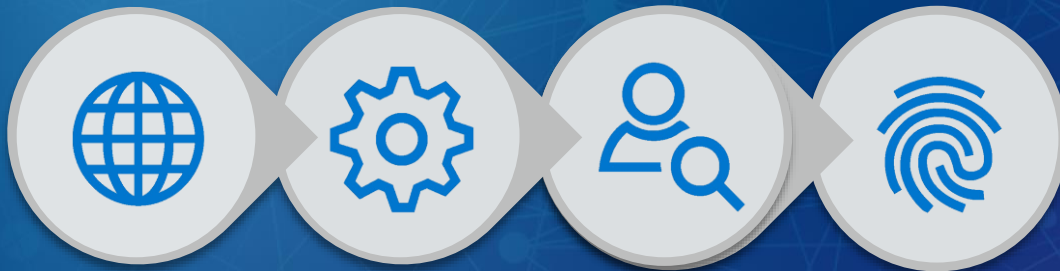
- Метаданные файла
- Метаданные документов и
- Содержимое документа
- Данные не отправляются в облако для анализа

Как работает CyberSense

Машинное обучение обеспечивает раннее обнаружение и быстрое восстановление после кибератаки

АНАЛИТИКА БЕЗОПАСНОСТИ

Более 100 статистических данных,
свидетельствующих о кибератаке



КОМПЛЕКСНЫЙ ИНДЕКС

Изменения в
содержании с течением
времени

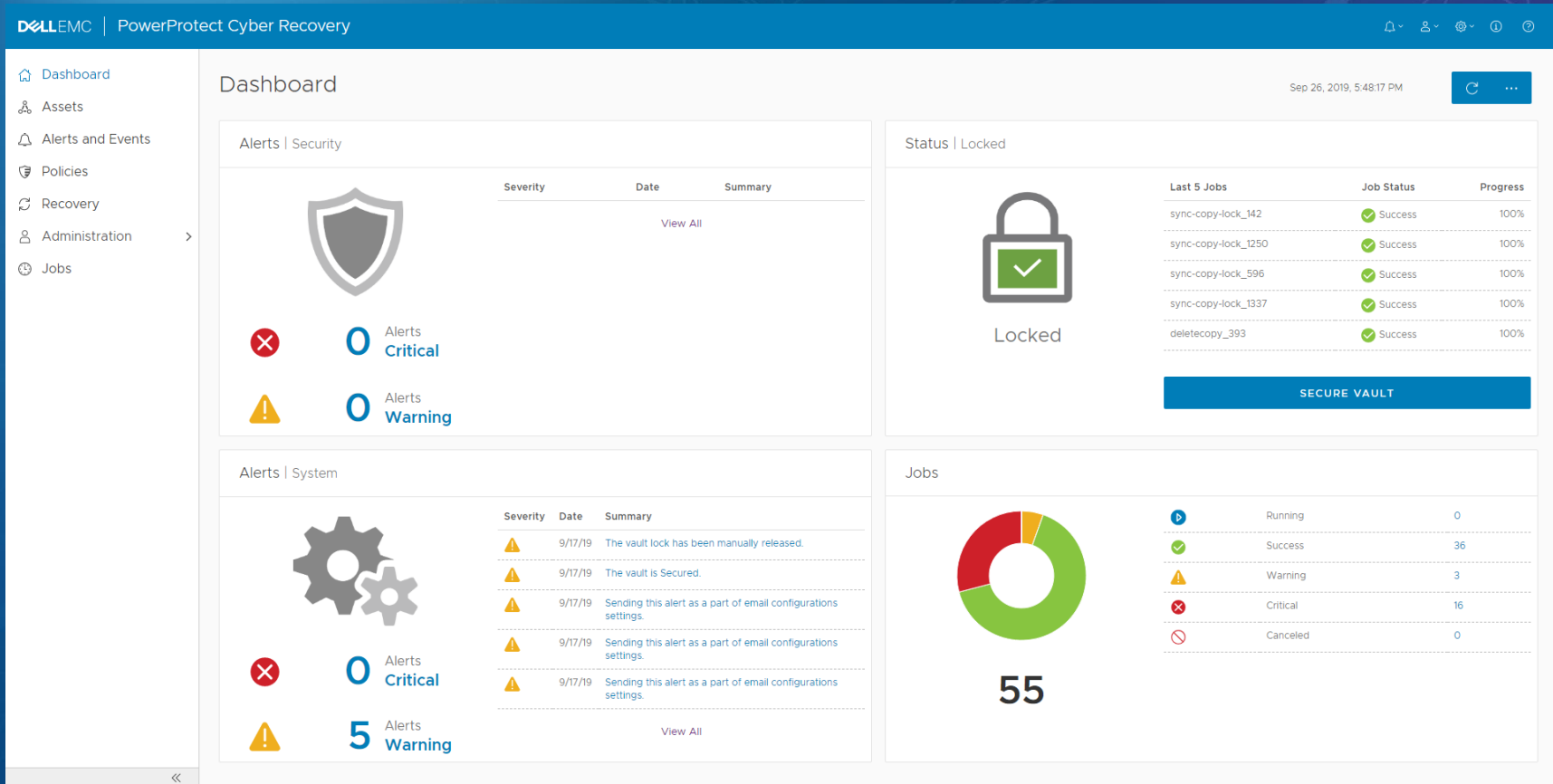
МАШИННОЕ ОБУЧЕНИЕ

Обучено на тысячах троянов и
более 20 векторах атак

Кибер-восстановление с CyberSense

- ✓ Уведомление о векторе атаки
- ✓ Программы-вымогатели
- ✓ Сведения о поврежденном файле
- ✓ Изменение/удаление данных
- ✓ Взломанные учетные записи пользователей
- ✓ Взломанные исполняемые файлы
- ✓ Восстановление последней исправной копии

Cyber Recovery UI



Отчет о кибервосстановлении

- Анализ более 100 статистических данных с использованием обученных алгоритмов машинного обучения
 - Анализ изменения данных
 - Энтропия
 - Сходство
 - Удаления
 - Повреждение файла
 - Несоответствие типа файла
 - Расширения программ-вымогателей
 - И более...
- Определение конкретного вектора атаки

L23		P56	
A	B	A	B
1 Backup Client Type	1	29 Created Ransomware Unique Count	14341
2 Backup Server	sa02.test.indexengines.com	30 Created Unique Backupset File Count	15200
3 Backup Time	1519150129	31 Created Unique File Count	15200
4 Backup Type	260	32 Deleted Entropy Threshold	3006
5 Backupset ID	sa02.test.indexengines.com	33 Deleted File Count	76854
6 Backupset Root Path	D:/	34 Deleted Mean Entropy	73.411903
7 Changed File Count	248	35 Deleted Mean File Size	358461
8 Changed File Type Count	6	36 Deleted Ransomware Extension Count	388
9 Changed Mean Similarity	71.274902	37 Prior Backup Size	30783918080
10 Changed Prior Entropy Threshold	3	38 Prior Corrupt File Count	201
11 Changed Prior Mean Entropy	40.4758	39 Prior Entropy Threshold	3672
12 Changed Prior Mean Size	20935916	40 Prior File Count	184179
13 Changed Prior Unique Count	238	41 Prior File Type Mismatch Count	0
14 Changed Prior-Deleted Mean Entropy		42 Prior Mean Entropy	61
15 Changed Ransomware Filter Count	0	43 Prior Mean File Size	304981
16 Changed This Entropy Threshold	4	44 Prior Ransomware Extension Count	17781
17 Changed This Mean Entropy	40.608898	45 Prior Unique File Count	137704
18 Changed This Mean Size	22924626	46 This Backup Size	31351859200
19 Changed This Unique Count	238	47 This Corrupt File Count	17
20 Changed This-Created Mean Entropy		48 This Entropy Threshold	14503
21 Created Entropy Threshold	13836	49 This File Count	122686
22 Created File Count	15361	50 This File Type Mismatch Count	0
23 Created Mean Entropy	95.895203	51 This Mean Entropy	57.639099
24 Created Mean File Size	1487063	52 This Mean File Size	423504
25 Created Ransomware Entropy	98.587303	53 This Ransomware Extension Count	31734
26 Created Ransomware Entropy Threshold	13809	54 This Unique File Count	85387
27 Created Ransomware Extension Count	14341	55 Unchanged File Count	107077
28 Created Ransomware Unique Backupset Count	14341	56 Unchanged Mean Entropy	52.190399
29 Created Ransomware Unique Count	14341		192.168.17.245-08.17.2018
30 Created Unique Backupset File Count	15200	57 Values Label	04-11-23 AM 150
31 Created Unique File Count	15200	58 Infected	4
32 Deleted Entropy Threshold	3006	59 Data Issues	training limit=1.377715
33 Deleted File Count	76854	60 Model Version	3
34 Deleted Mean Entropy	73.411903		
35 Deleted Mean File Size	358461		
36 Deleted Ransomware Extension Count	388		
37 Prior Backup Size	30783918080		

Проблемы киберустойчивости сегодня

Программа-вымогатель теперь может быть самой большой угрозой для клиента!

Cyber Bunker отвечает на 3 главных вопроса:

- Что, если я был зашифрован?
- Меня шифруют?
- Как восстановить, если я зашифрован?

Основные выводы

1. Если у вас есть X данных — попросите поставщиков предоставить вам необходимую емкость (имея в виду, что количество данных X может соответствовать емкости Y)

Почему?

Цена! Стоимость охлаждения! Электричество!

Место в стойке! Стоимость технического обслуживания!

2. Запросите у поставщика совокупную стоимость владения (ТСО) (не только цену!)

Почему?

Гиперконвергентное решение может спасти ваш бизнес!

3. Проверьте стоимость и влияние простоя

4. Киберустойчивость — как вы защищены (резервного копирования НЕ ДОСТАТОЧНО!)



საქართველოს კირველი
ცენტრალური
ბანკი

Проект Active/Active растянутого кластера на DELL VxRail

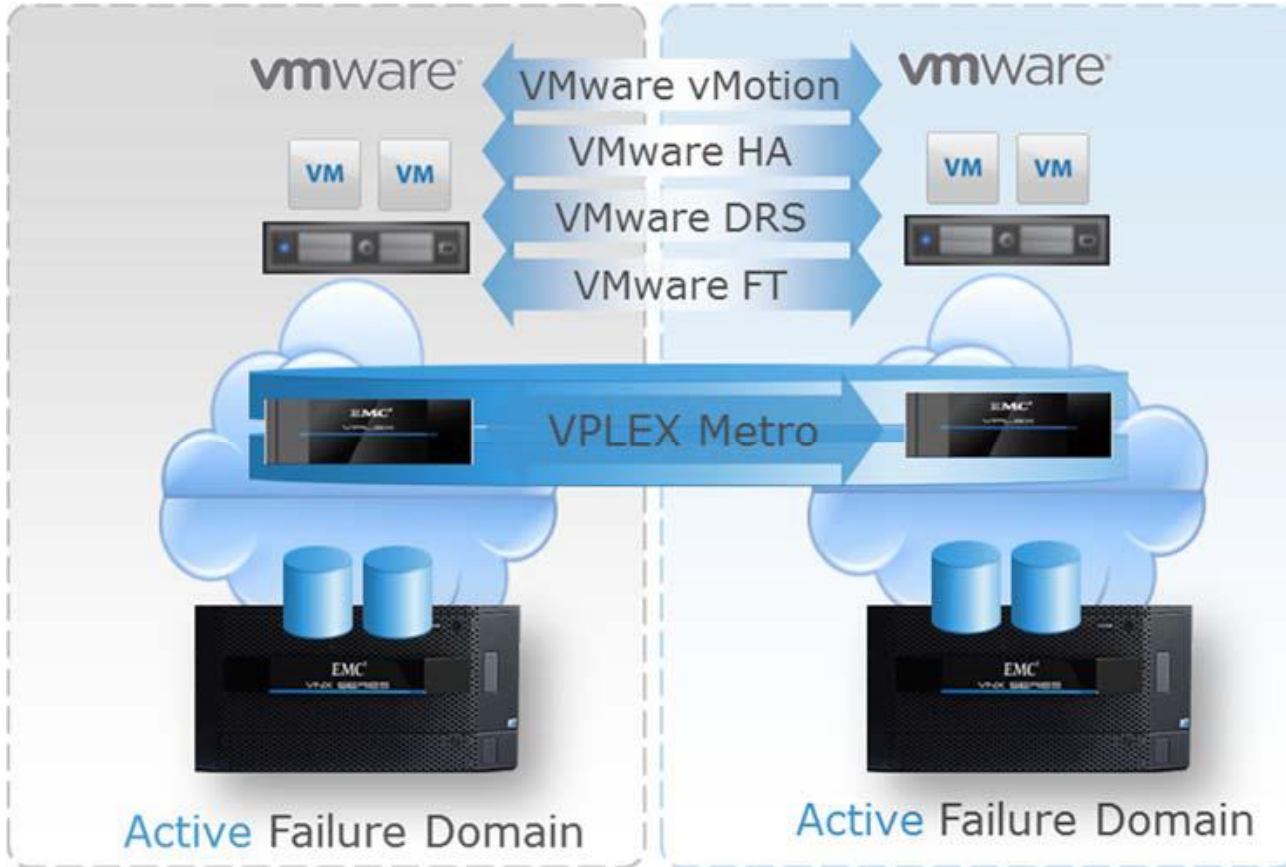


История успеха – Национальный Банк Грузии



საქართველოს კირველი
ცენტრალური
ბანკი

Существующая инфраструктура





Традиционная инфраструктура ЦОД



- Традиционная инфраструктура не оптимизирована для современных рабочих нагрузок.
- Трудно управлять и обслуживать устройства хранения данных
- Низкое внедрение автоматизации.



საქართველოს კირველი
ცენტრალური
ბანკი



Цель

Модернизации инфраструктуры со следующими атрибутами:

All Flash



Сокращение затрат

Стабильная и предсказуемая производительность

Поддержка облака



Предоставление услуг на основе политик

Ориентированный на виртуальные машины подход

Масштабирование



Масштабирование по мере роста

Управление меньшими ресурсами

Программно-
определяемый



Автоматизация выделения ресурсов

Программируемые службы данных

Тот же уровень доступности

Надежный



Зрелое, безопасное и надежное решение



საქართველოს კირველი
ცენტრალური
ბანკი



Решение

VxRail - HCI решение разработанное совместно Dell EMC & VMware

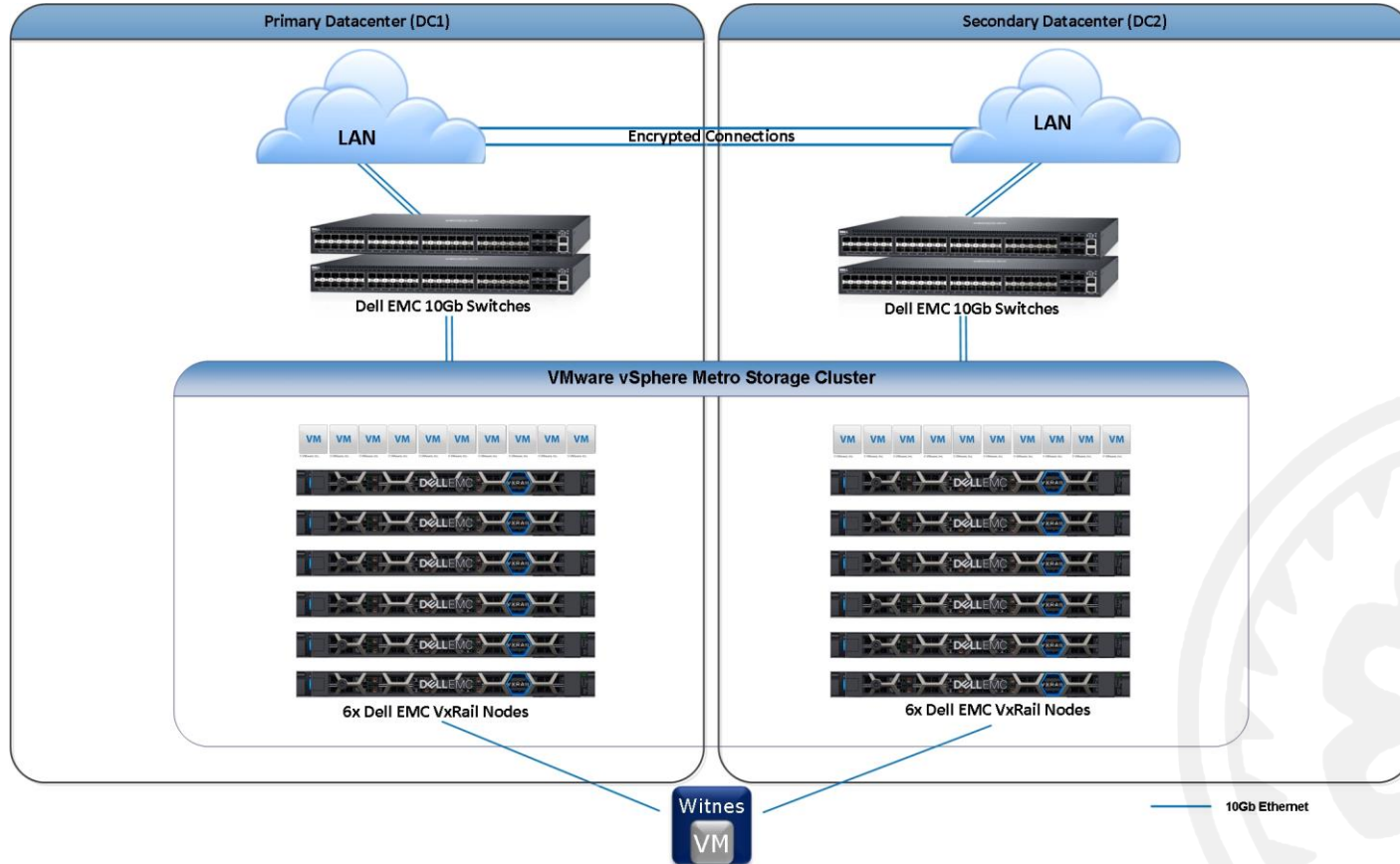




საქართველოს კირველი
ცენტრალური
ბანკი



Новое Metro-кластерное решение





საქართველოს კირველი
ცენტრალური
ბანკი



Переход на Software-Defined

COST EFFECTIVE- SYSTEMS DESIGN SHIFT



THEN

HYPER-CONVERGED



NOW



საქართველოს კირველი
ცენტრალური
ბანკი

Результаты

Производительность виртуальных машин с БД и приложениями значительно улучшилась.

Один простой способ управления состоянием и жизненным циклом всех компонентов гиперконвергентной инфраструктуры.

Упрощенный процесс развертывания и обновления — 2 дня для установки в стойку и стек + 2 дня для внедрения распределенного кластера. Обновления без прерывания работы.

Улучшенная непрерывность бизнеса и процесс аварийного восстановления.

Улучшенная масштабируемость и гибкость центра обработки данных — помогают удовлетворять внутренние потребности в других услугах по требованию или решениях для частных облачных вычислений.

Безопасность, доступность и целостность - VxRail предназначен для защиты центра обработки данных от современных кибератак. Тот же уровень доступности, что и у VPLEX.

Единая точка поддержки от одного поставщика — Dell EMC



DELL Technologies



საქართველოს კირველი
უნივერსიტეტი
ბაზი

Тесты производительности в IOPS

Две площадки, Raid-5 с Дедупликацией и Компрессией

Datastore: VxRail-vSAN-Datastore

=====

Version: vdbench50407

Run Def: RD=run1; I/O rate: Uncontrolled MAX; elapsed=360; For

loops: None

VMs = 16

IOPS = 112534.50 IOPS

THROUGHPUT = 439.60 MB/s

LATENCY = 1.1342 ms

R_LATENCY = 0.5816 ms

W_LATENCY = 2.4215 ms

95%tile_LAT = 2.7152 ms

=====

Resource Usage:

CPU USAGE = 13.66%

RAM USAGE = 9.17%

VSAN PCPU USAGE = 4.7142%

=====



საქართველოს კირველი
ცენტრალური
ბანკი



Новое решение аварийного
восстановления в качестве бонуса



DELLTechnologies