COMMVAULT | Be ready

Безопасность при удаленной работе

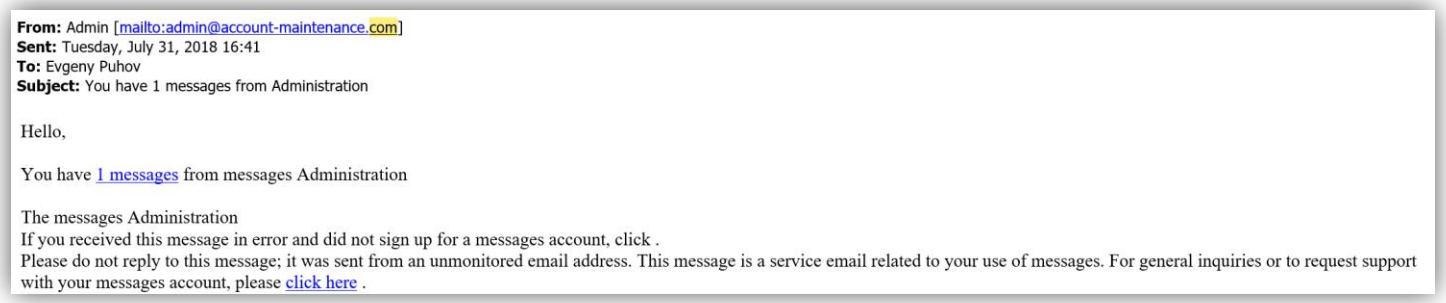
Консультант

Евгений Пухов

epuhov@commvault.com

Риски удаленного доступа к данным

1. **BYOD**
2. **Преднамеренные воздействия.** Различное вредоносное ПО, фишинг
3. **Непреднамеренные действия.** Случайное удаление данных, почты, ошибки синхронизации с облаками



From: Admin [mailto:admin@account-maintenance.com]
Sent: Tuesday, July 31, 2018 16:41
To: Evgeny Puhov
Subject: You have 1 messages from Administration

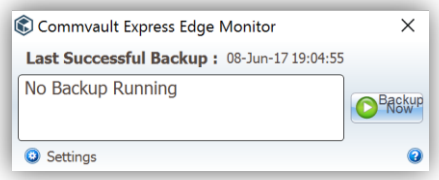
Hello,

You have 1 messages from messages Administration

The messages Administration
If you received this message in error and did not sign up for a messages account, click .
Please do not reply to this message; it was sent from an unmonitored email address. This message is a service email related to your use of messages. For general inquiries or to request support with your messages account, please click here .

Защита ПК конечных пользователей

Сбор данных с клиента с ПК пользователей



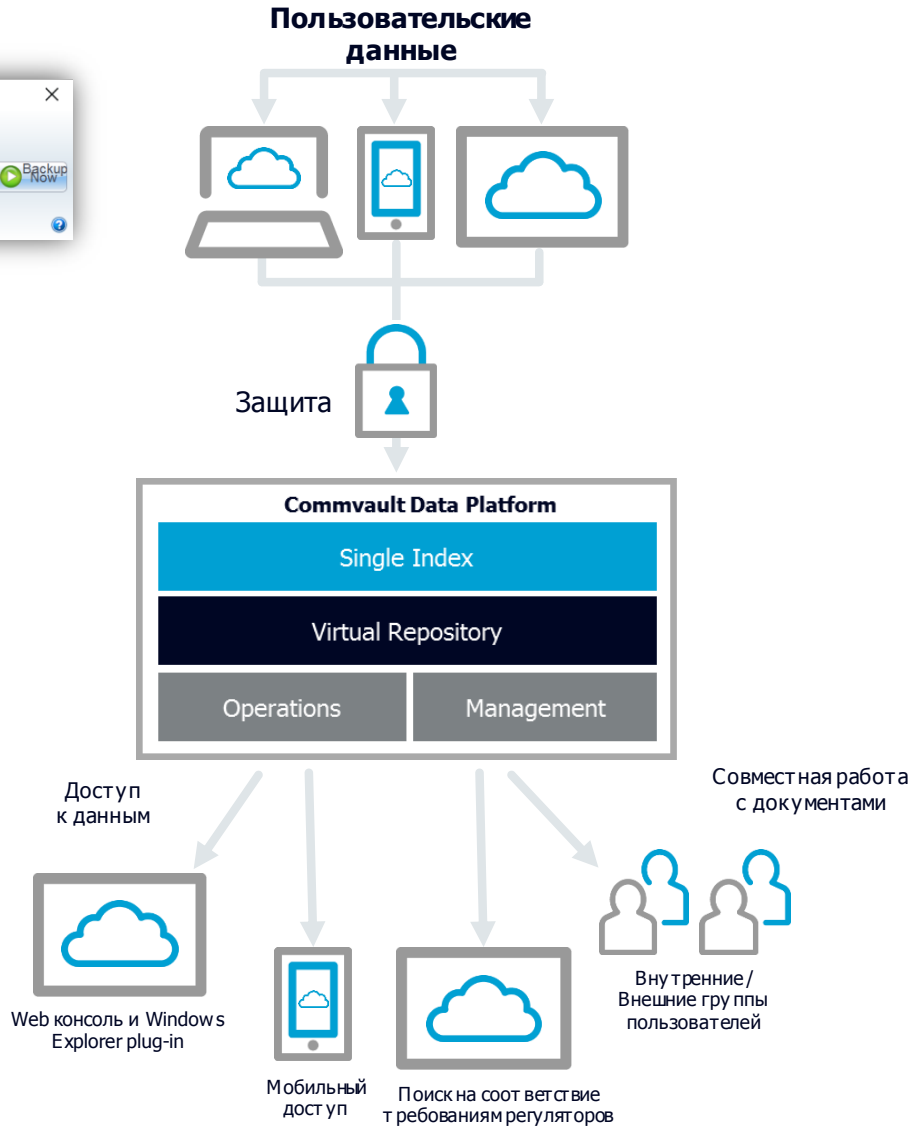
- Без настроек на клиенте. Через веб портал.
- Source-side дедупликация с инкрементальными копиями минимизирует трафик
- Автоматическое динамическое расписание, ограничение пропускной способности
- Доступ к своим резервным копиям через web портал,Explorer plug in, Finder plug in, приложения для iOs, Android

Безопасность

- Аномальная активность
- Безопасные сетевые соединения
- Двух-факторная авторизация, SSO + SAML и различные ролевые модели доступа

Data loss prevention

- Выборочное шифрование данных
- Выборочное уничтожение информации с украденных или утерянных ПК
- Геолокация ПК, в том числе утерянных



Защита ПК конечных пользователей от Ransomware

Ранеее обнаружение Ransomware

- Технология Honeypot trap

Данные в облаке также могут быть заражены Ransomware

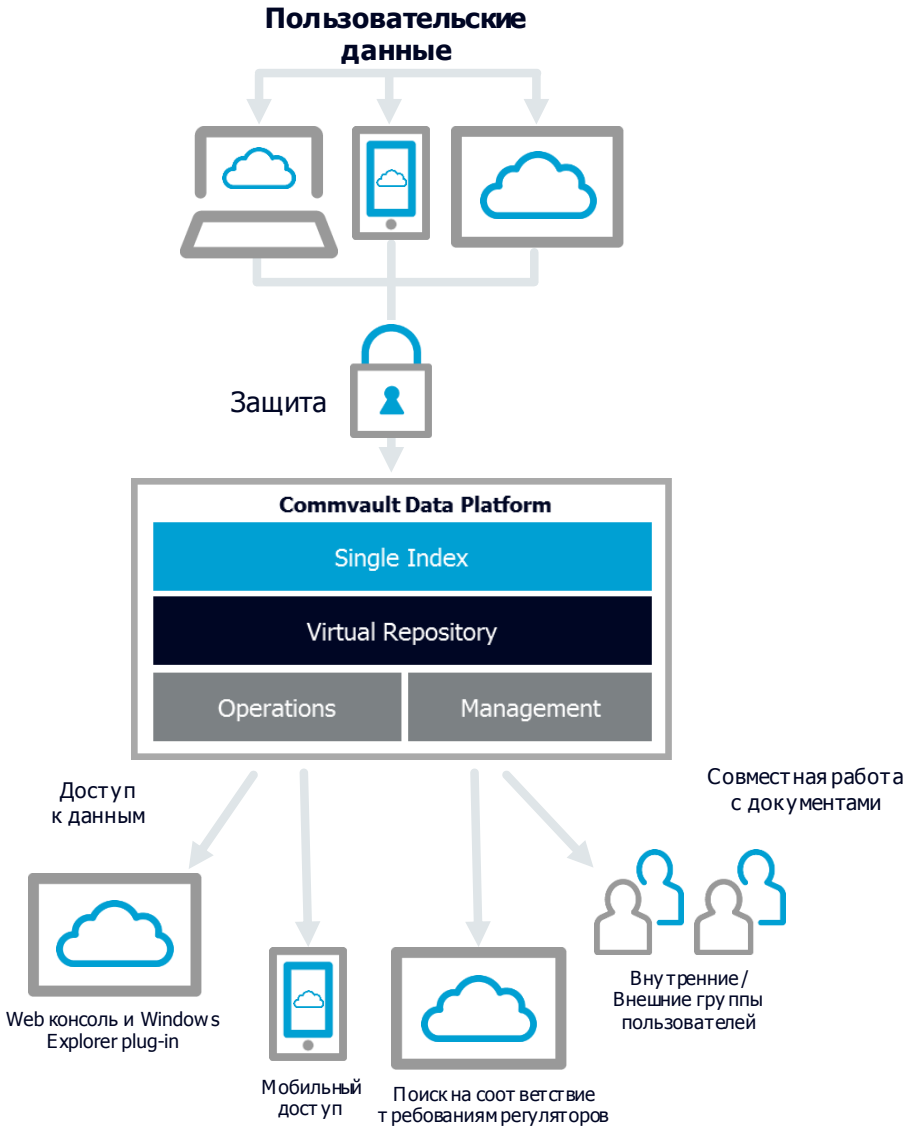
- Синхронизация с «облаком» небезопасна! Испорченный контент может повредить данные в облаке при синхронизации
- Зараженные файлы через синхронизацию и веб - ссылки могут проникать и распространяться через интранет прозрачно для ИБ

Восстановление после вирусной атаки силами Commvault

- Изоляция точки заражения во времени
- Point-in-time восстановление
- Self - service восстановление предыдущих версий через пользователельский web интерфейс

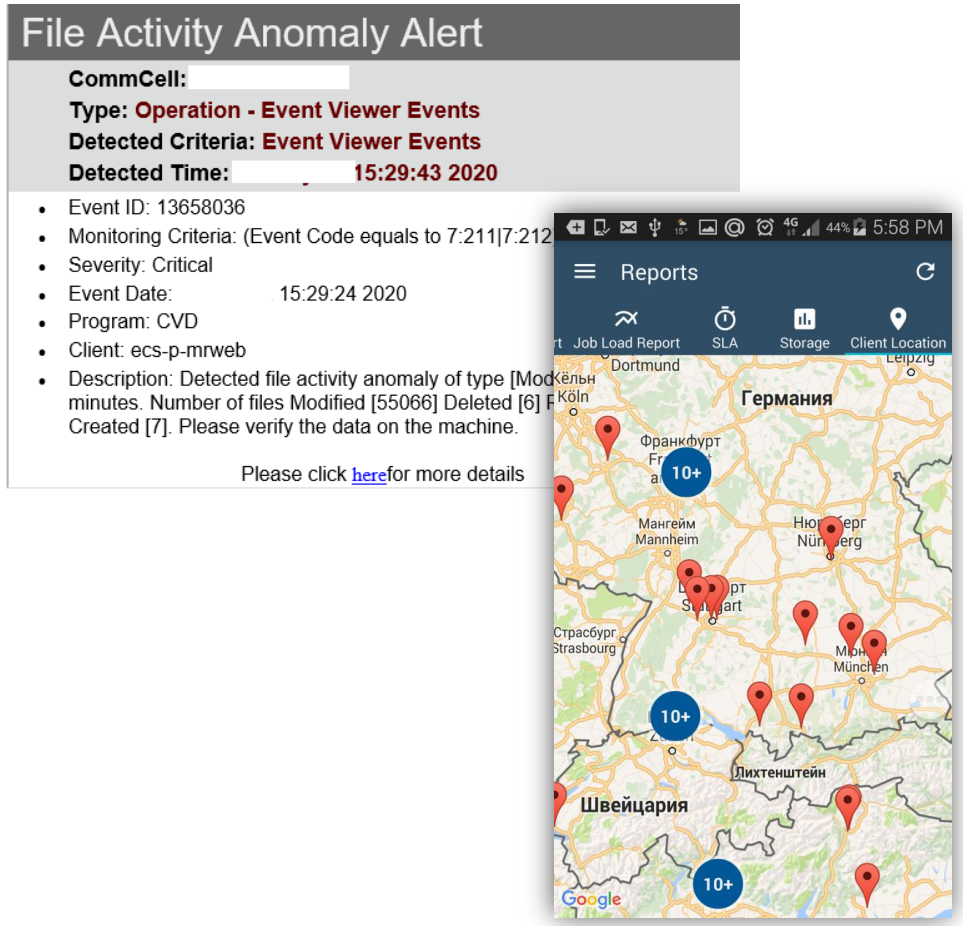
Защита сервисов Commvault от вредоносного ПО

- Создание Offline копий данных
- Хранить РК только на выделенных под Commvault томах. Защита томов Commvault от перезаписи

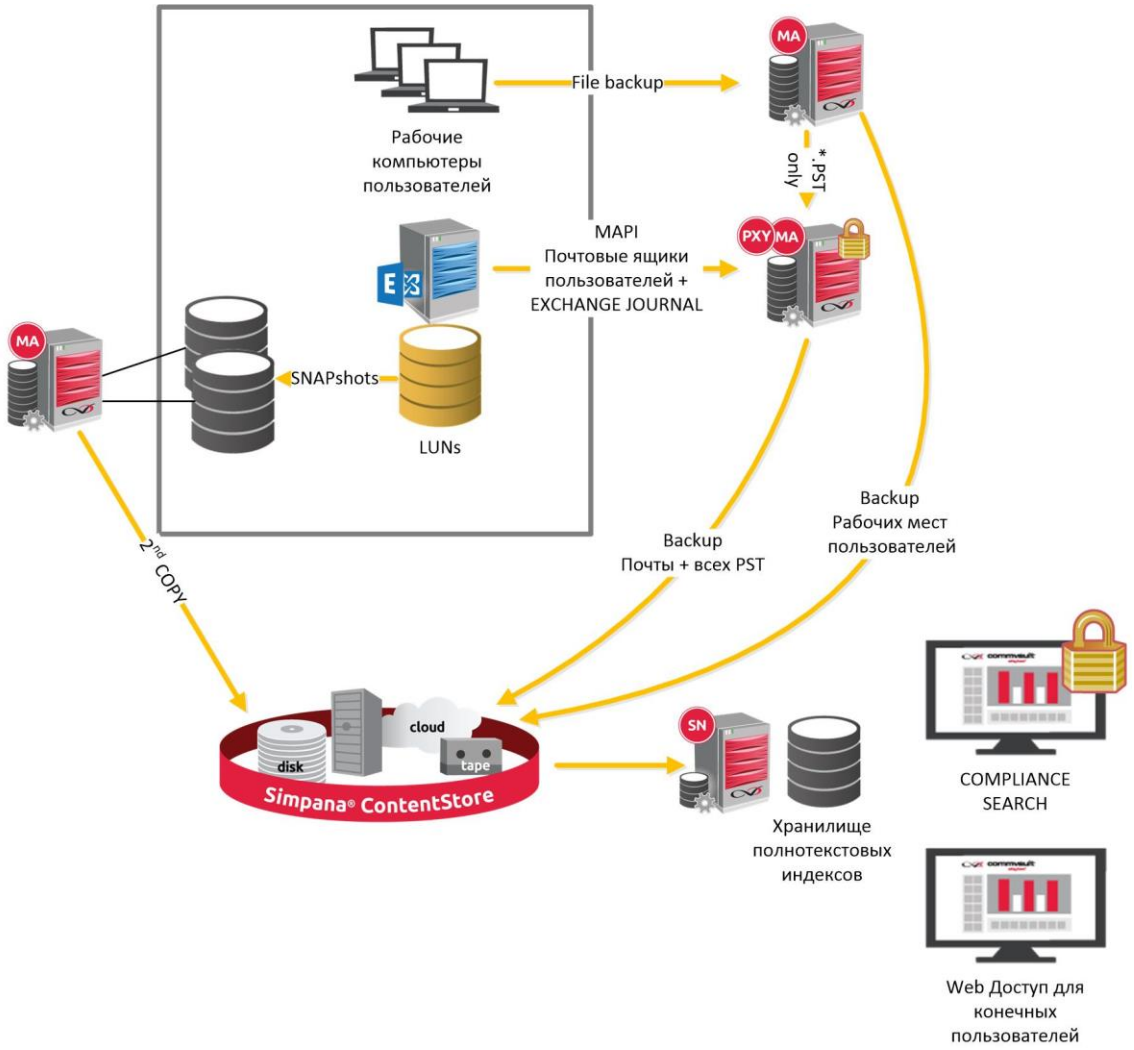


Обнаружение аномальной активности

- Слишком много новых измененных данных (на блочном уровне)
- Слишком частые ошибки подключения устройства
- Необычно много новых/измененных файлов от конкретного пользователя или группы
- Необычная локация пользователя
- Защита от Ransomware. Технология Honeypot trap (файл – приманка)
- В дополнение к DLP системам COMMVAULT обеспечивает анализ нарушений на длительных временных интервалах



Пример решения : Защита данных + ИБ



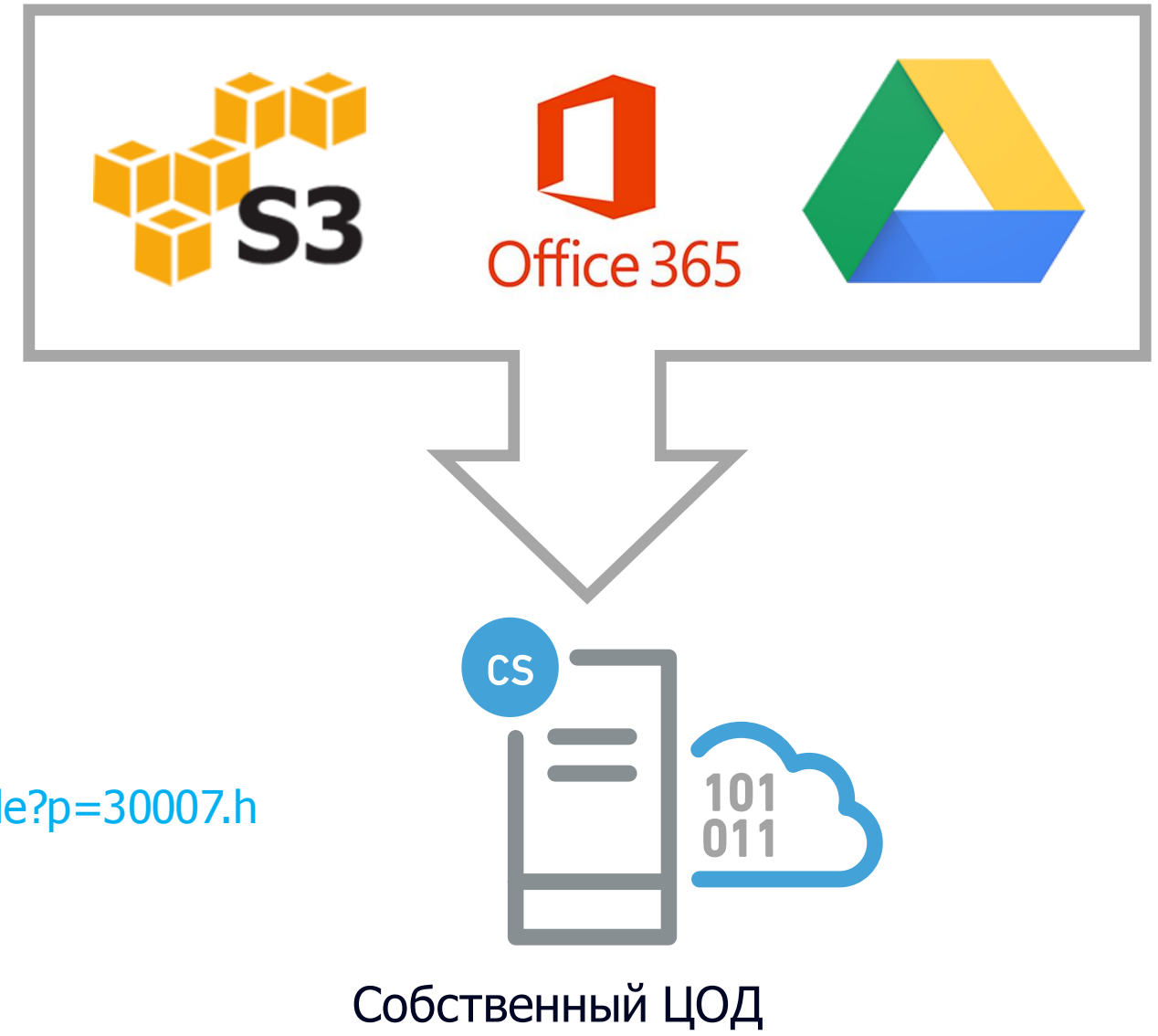
- Сбор всех документов вместе с *.pst архивами с рабочих станций (в том числе незаметно для пользователей)
- Сбор журнала Exchange
- Контекстное индексирование
- Анализ на предмет ненадлежащего контента, ненадлежащих адресатов и т.п.

Прямой путь **ИЗ облаков.** Архивирование данных

Поддерживаемые облачные провайдеры

- Office 365
- Gsuite (Gmail/Gdrive)
- Azure blob storage
- Amazon S3 + совместимые
- Amazon RDS (database)
- Oracle cloud storage
- Azure SQL
- И др

http://docs.commvault.com/commvault/v11/article?p=30007.htm



Собственный ЦОД

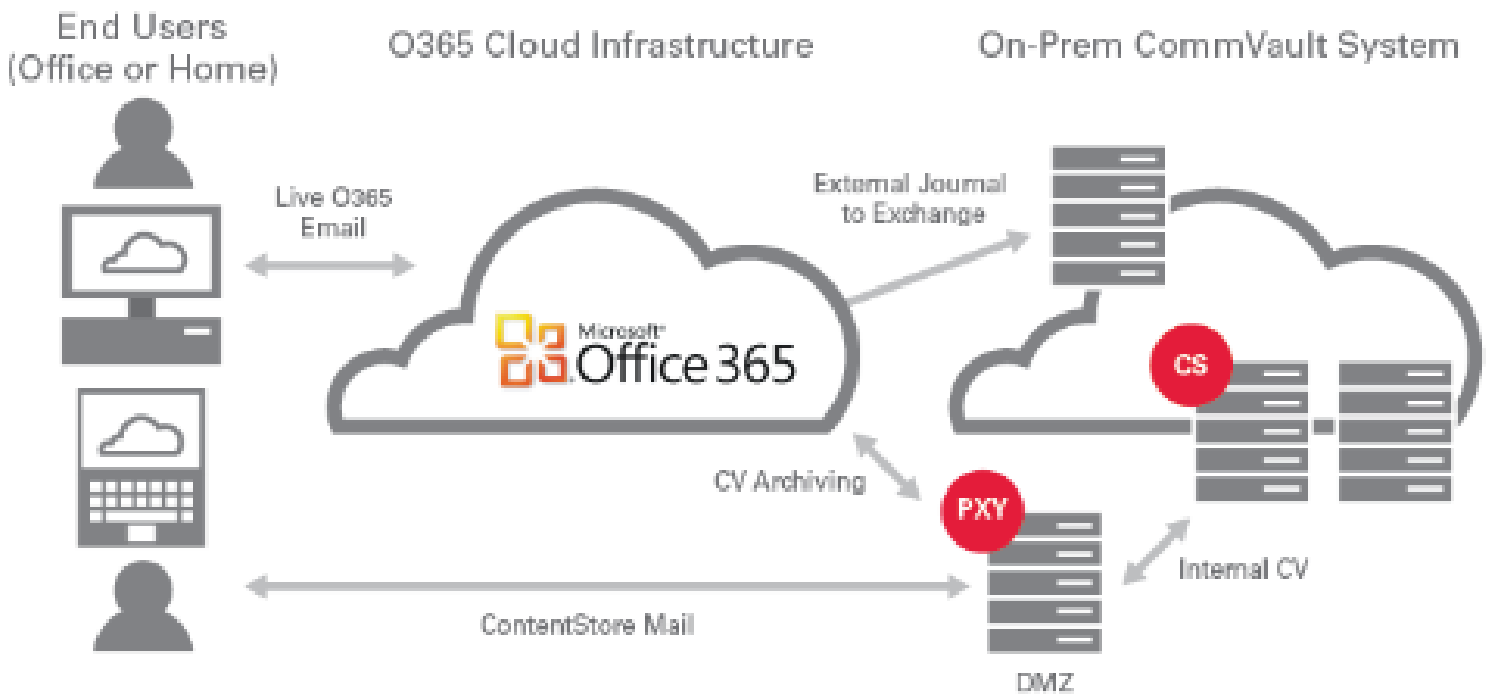
Интеграция с Office 365. Google mail. OneDrive

O365 Integration

- Архив и журнал O365 по MAPI
- Полностью аналогично и прозрачно как и Exchange on-premise
- Контекстный поиск
- НЕ зависит от работоспособности облака

Почему 0365 лучше в связке с Commvault

- Требования регулятора.. Персональные данные и трансграничная передача!
- Гранулярность восстановления и Retention по письмам
- Legal Hold. Read-only content
- В любой момент можно уйти с O365
- Независимость от сбоев O365 и каналов связи

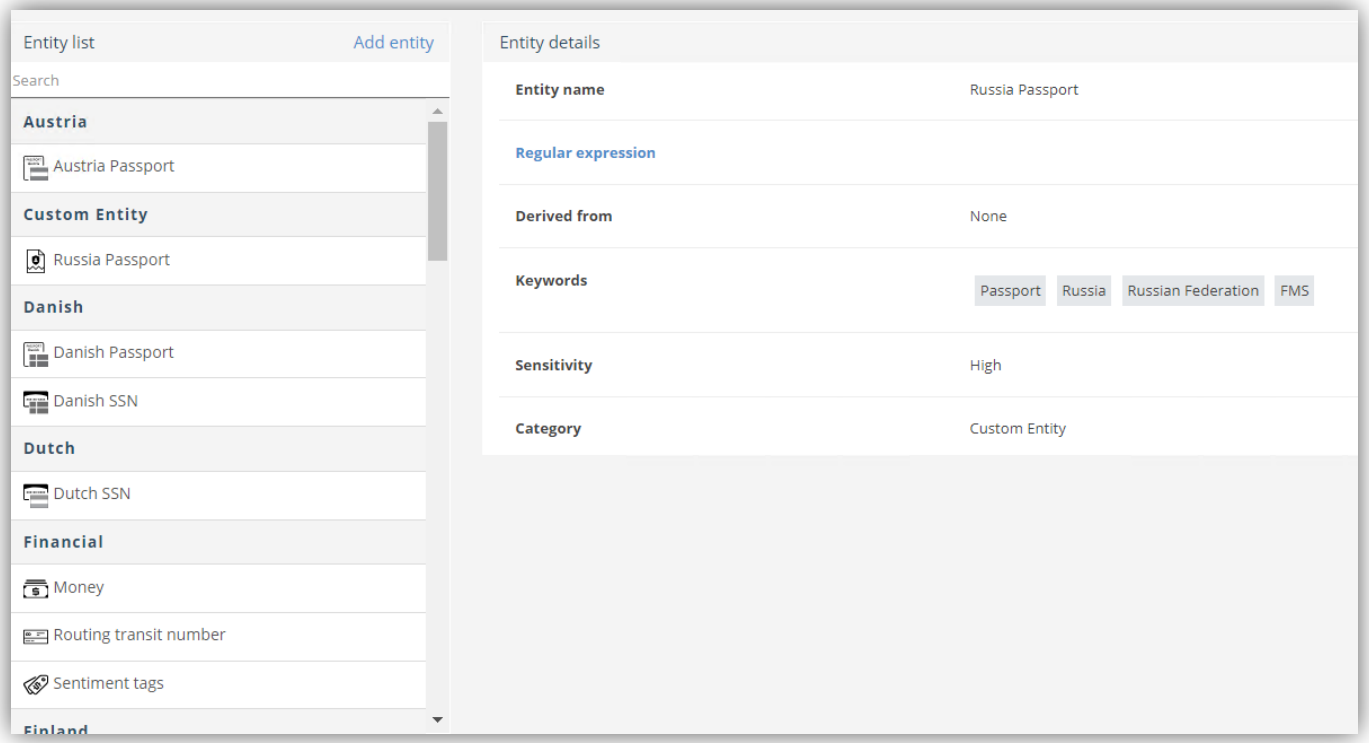


Фильтрация Персональных данных

Что мы умеем:

После полнотекстового индексирования выделить следующие типы информации

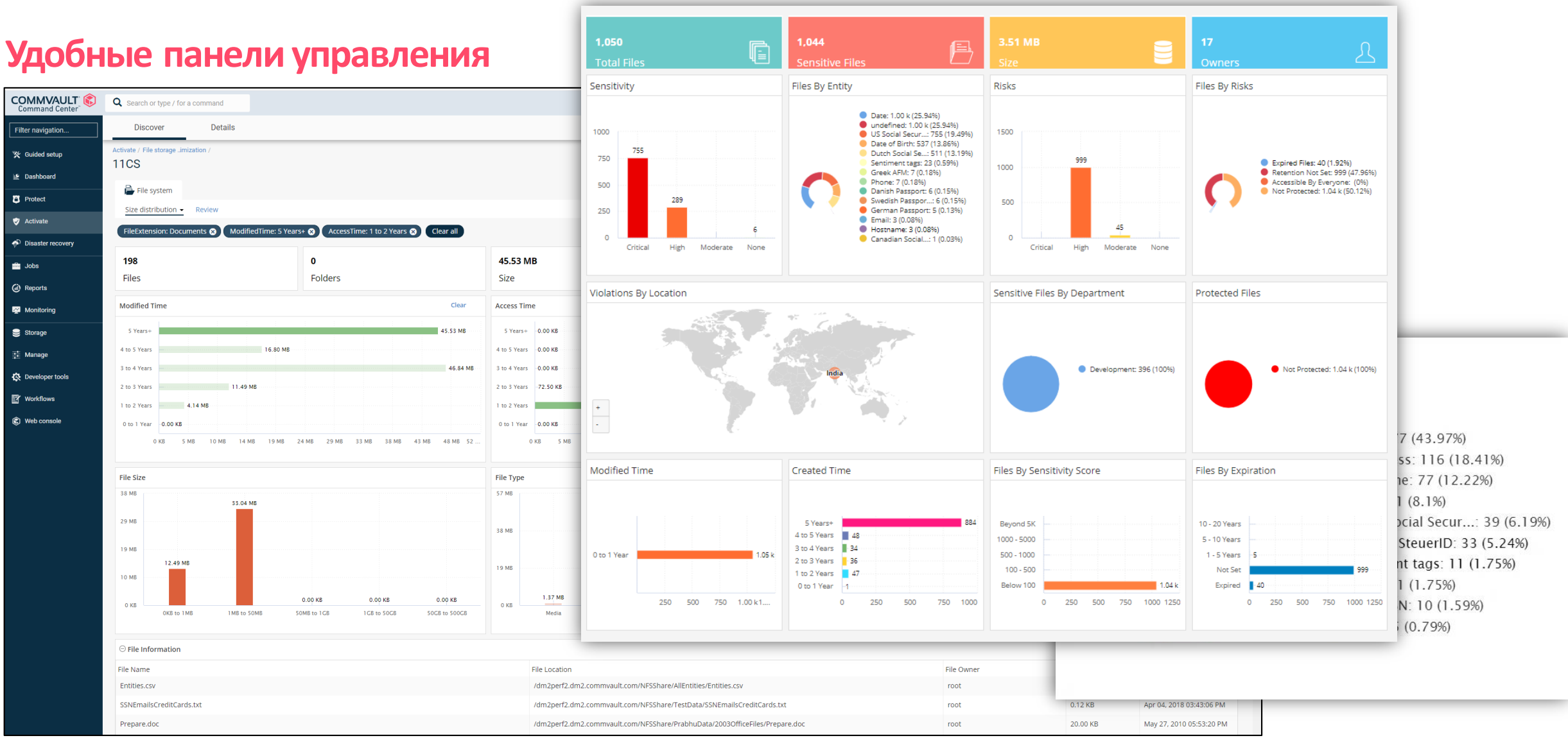
- Электронные адреса и ссылки
- Номера кредитных карт
- Телефоны
- Что угодно другое в любой комбинации с применением ML



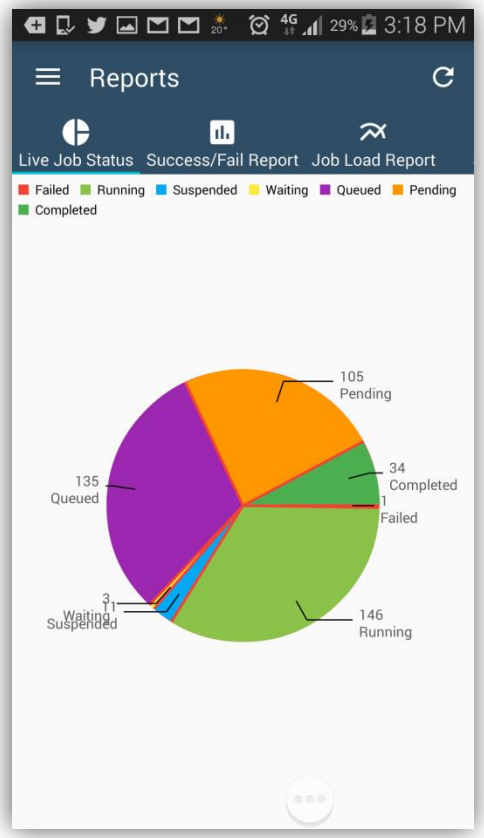
Зачем это нужно:

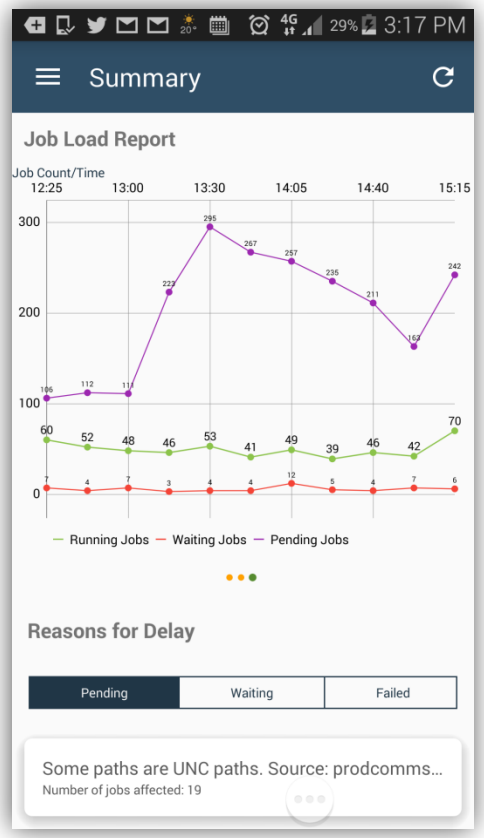
- Соответствия требованиям регуляторов. 149-ФЗ, 152-ФЗ, трансграничная передача, PCI DSS

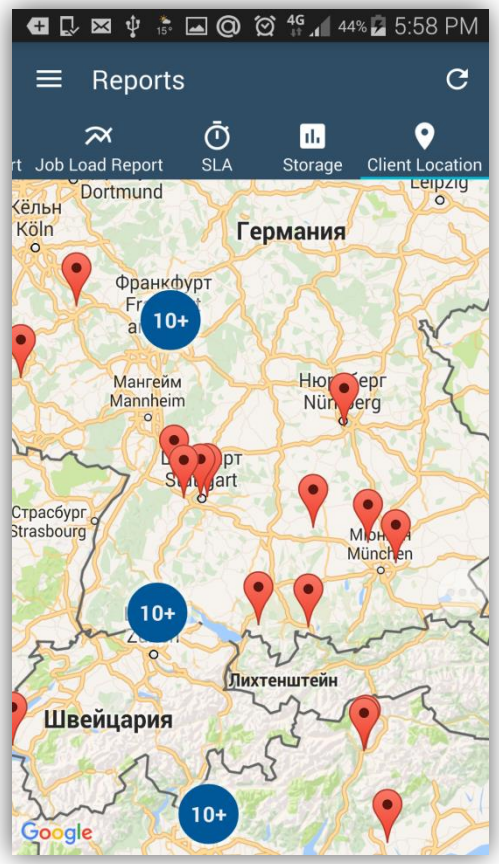
Удобные панели управления



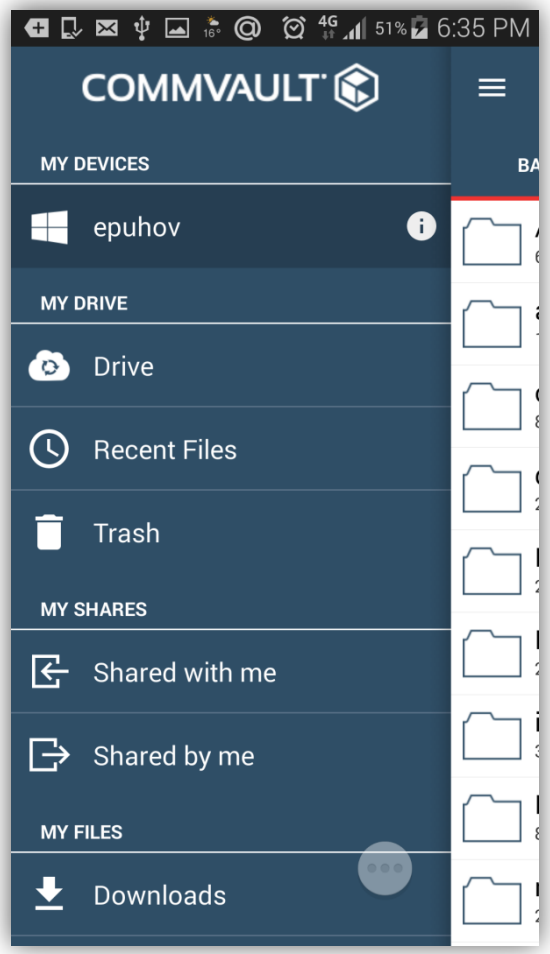
Мобильное приложение для мониторинга РК

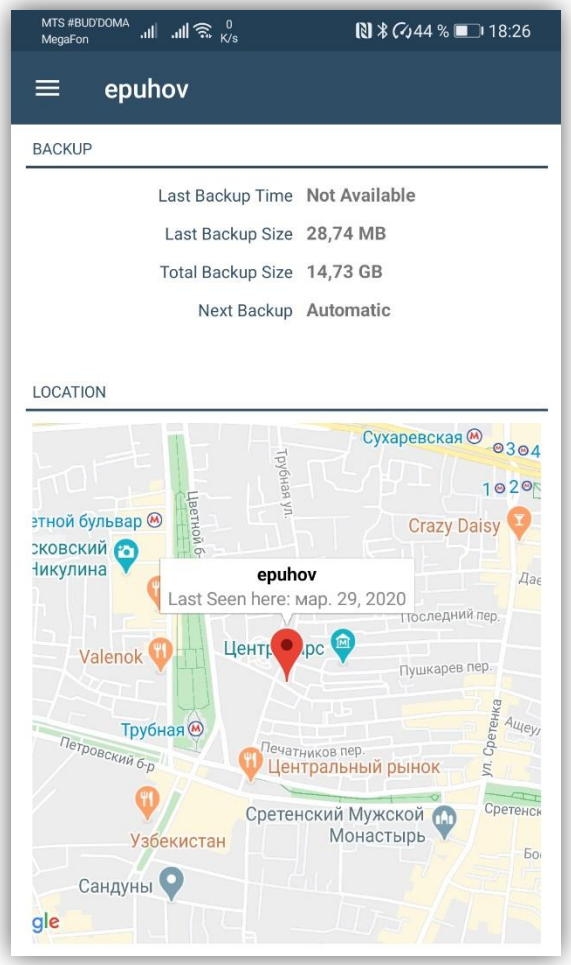


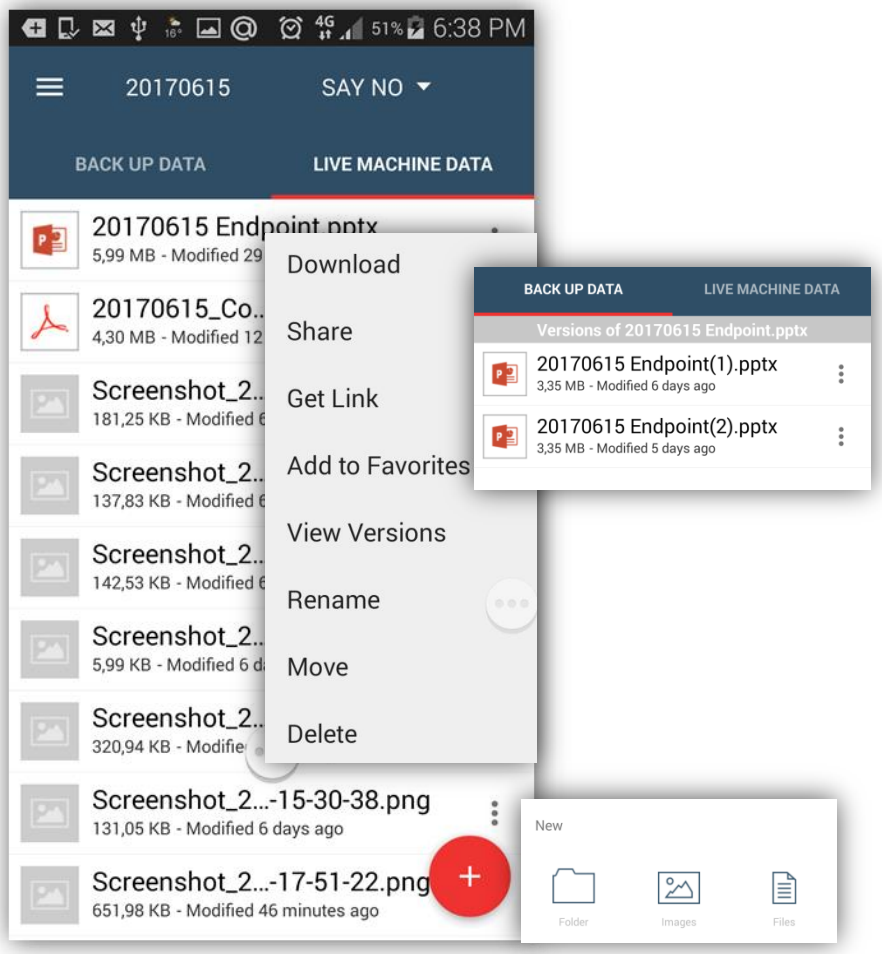




Мобильное приложение для доступа к данным



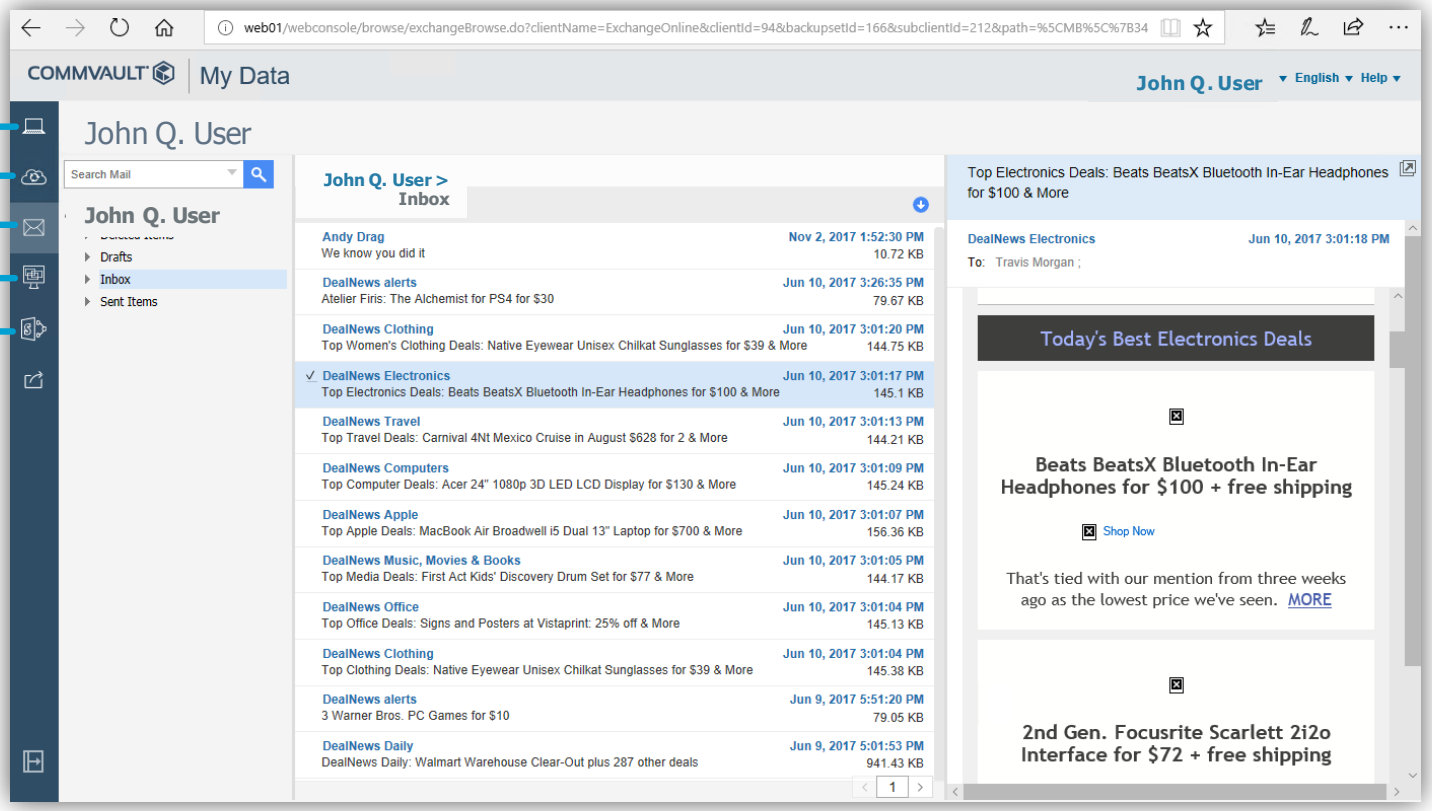




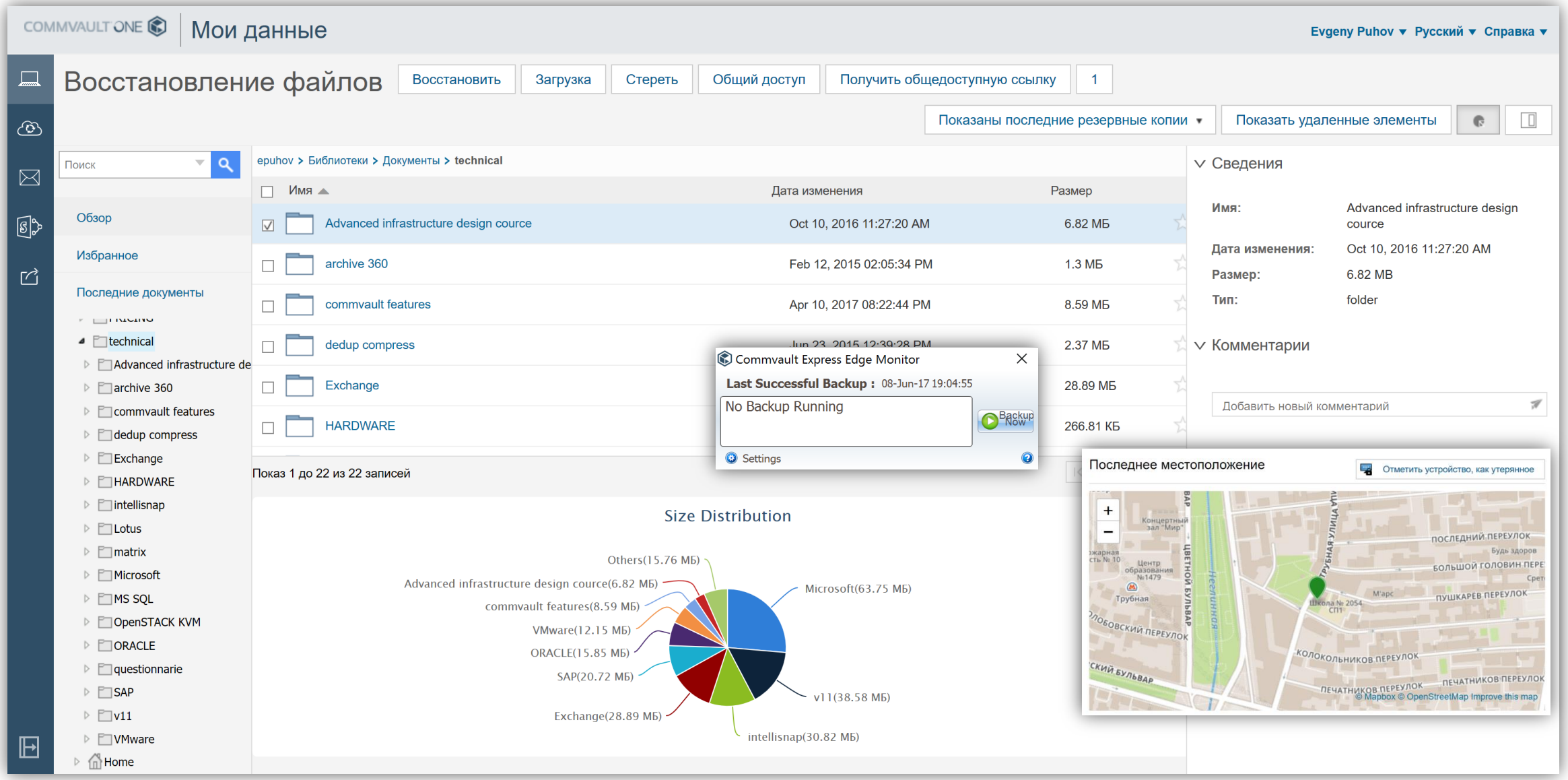
Веб Консоль конечного пользователя

Панель самообслуживания. Поиск, загрузка, управление ВМ

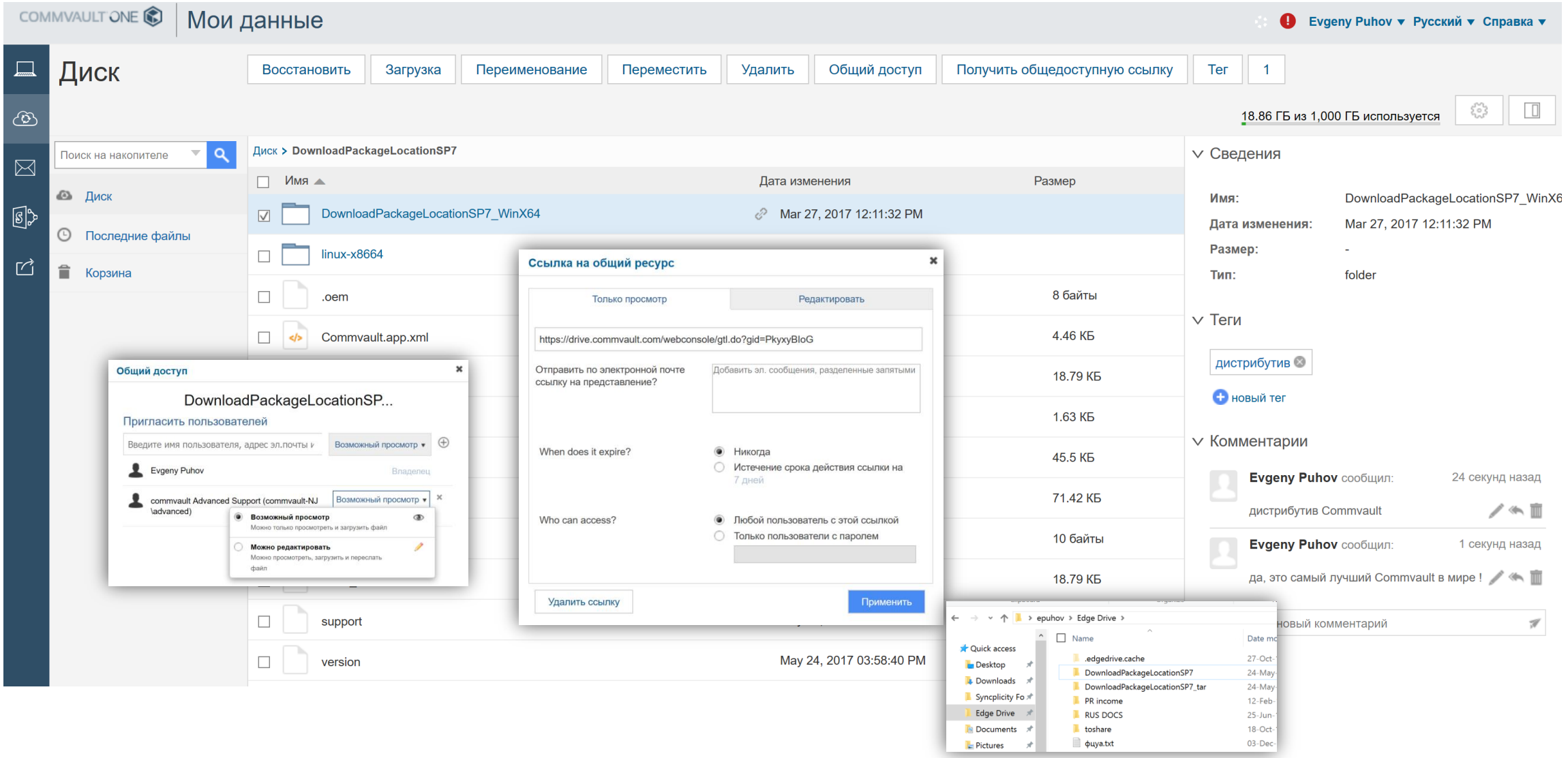
Laptop backup
Edge Drive
Email
Virtual machines
SharePoint



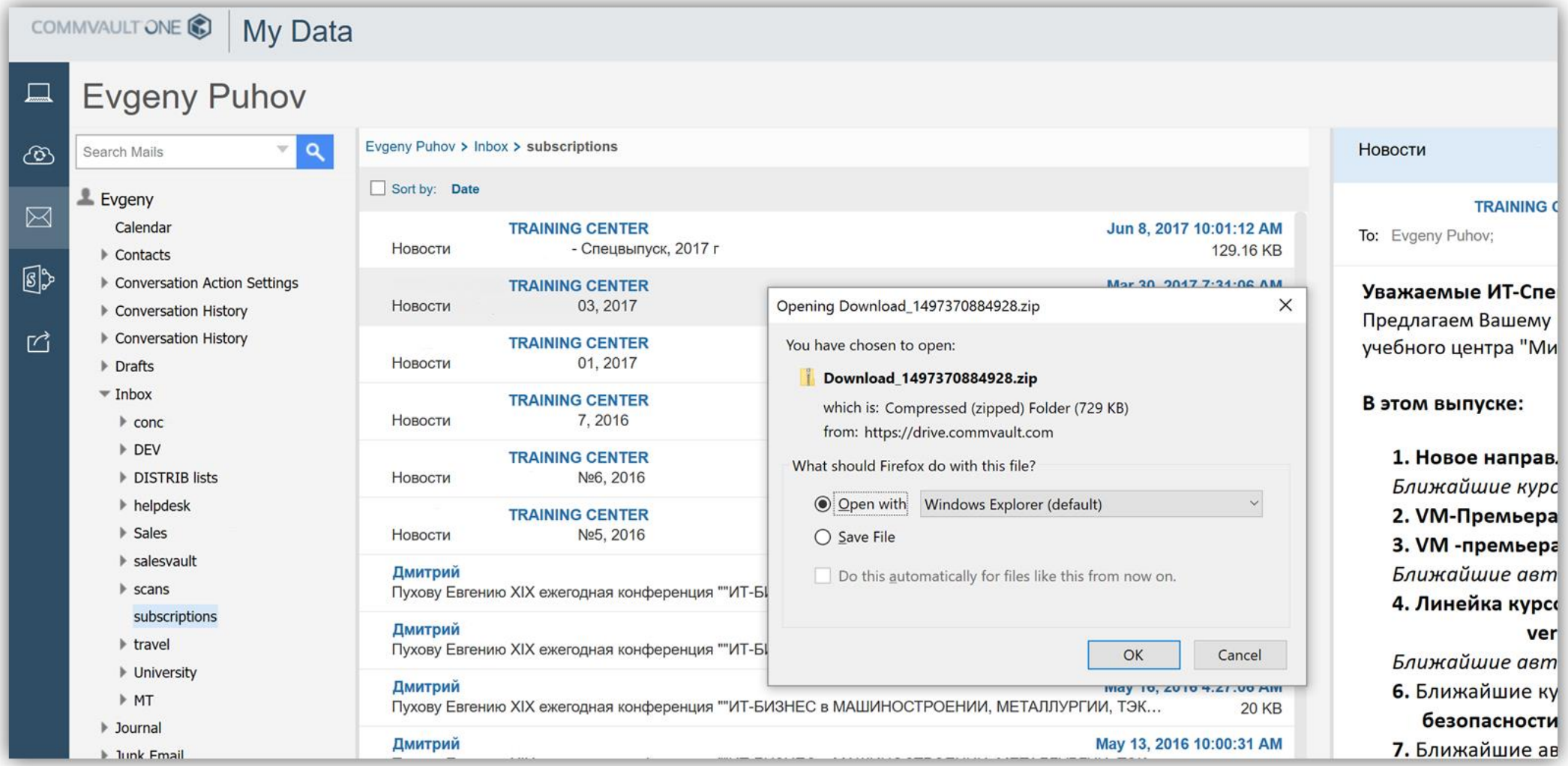
Web интерфейс Commvault Endpoint. Резервные копии



Web интерфейс Commvault Endpoint. EDGE drive



Web интерфейс Commvault Endpoint. Почта



Информационная безопасность. Метод Commmvault

Резервное копирование при правильной реализации – 100% гарантия сохранности данных

- Разделение ролей : **администратор ИБ – Data Protection Officer** (мониторинг содержимого и активности) , **администратор РК** (копирование и восстановление данных и приложений)
- Защита хранилища РК от перезаписи сторонними приложениями
- Использование нестандартных IP портов для обмена данными
- Защита от Ransomware. Технология Honeypot trap
- Физическое удаление данных с носителя CVDISKERASER
- В дополнение к DLP системам обеспечивает анализ нарушений на длительных временных интервалах
- Выборочное шифрование данных

COMMVAULT | Be ready™

Спасибо за внимание!