



# Безопасность при удаленной работе

**Консультант**

Евгений Пухов

[epuhov@commvault.com](mailto: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

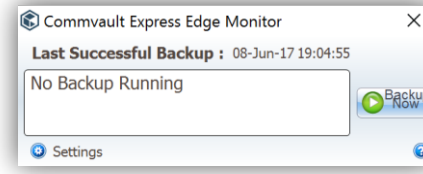
If you received this message in error and did not sign up for a messages account, click .

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

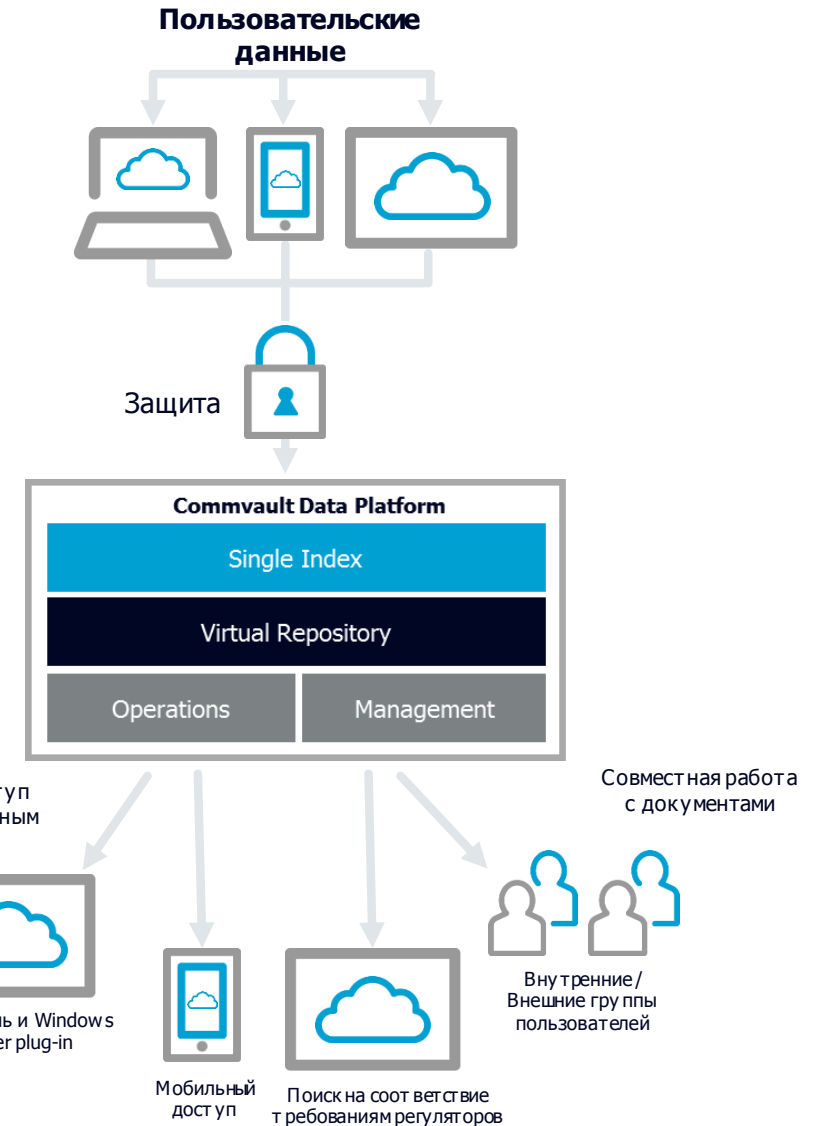


## Безопасность

- 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

### Раннее обнаружение Ransomware

- Технология Honeypot trap

### Данные в облаке также могут быть заражены Ransomware

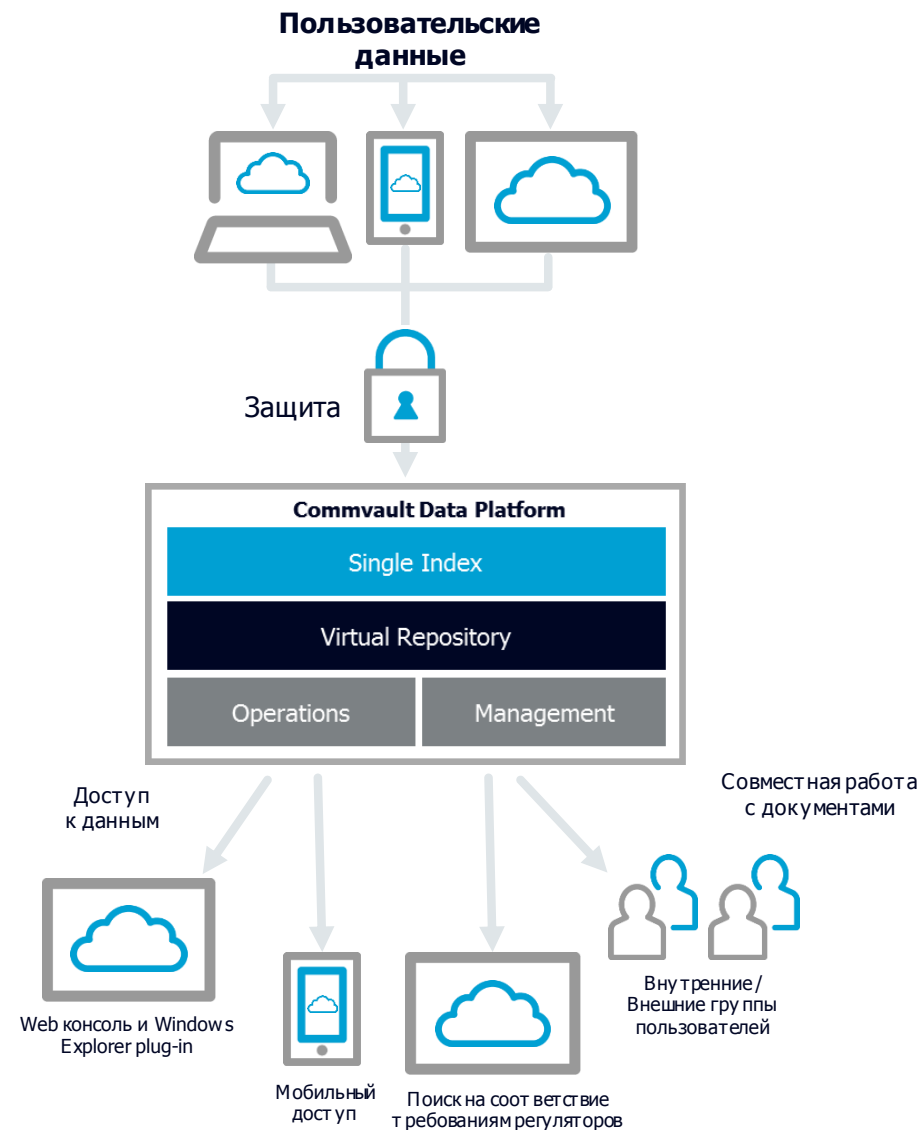
- Синхронизация с «облаком» небезопасна! Испорченный контент может повредить данные в облаке при синхронизации
- Зараженные файлы через синхронизацию и веб - ссылки могут проникать и распространяться через интранет прозрачно для ИБ

### Восстановление после вирусной атаки силами Commvault

- Изоляция точки заражения во времени
- Point-in-time восстановление
- Self - service восстановление предыдущих версий через пользовательский 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

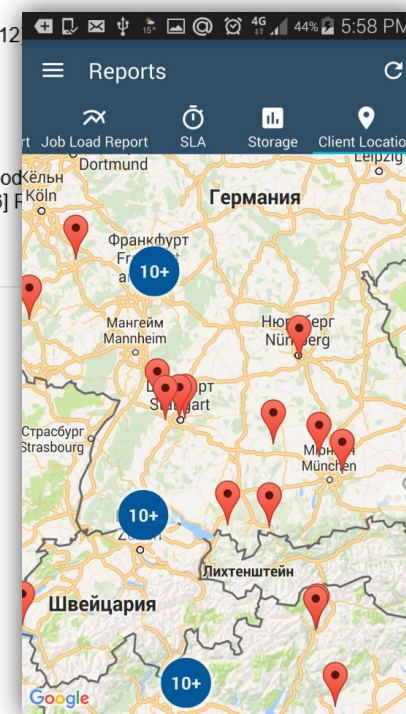
- Слишком много новых измененных данных ( на блочном уровне )
- Слишком частые ошибки подключения устройства
- Необычно много новых/измененных файлов от конкретного пользователя или группы
- Необычная локация пользователя
- Защита от Ransomware. Технология Honeypot trap (файл – приманка)
- В дополнение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

### File Activity Anomaly Alert

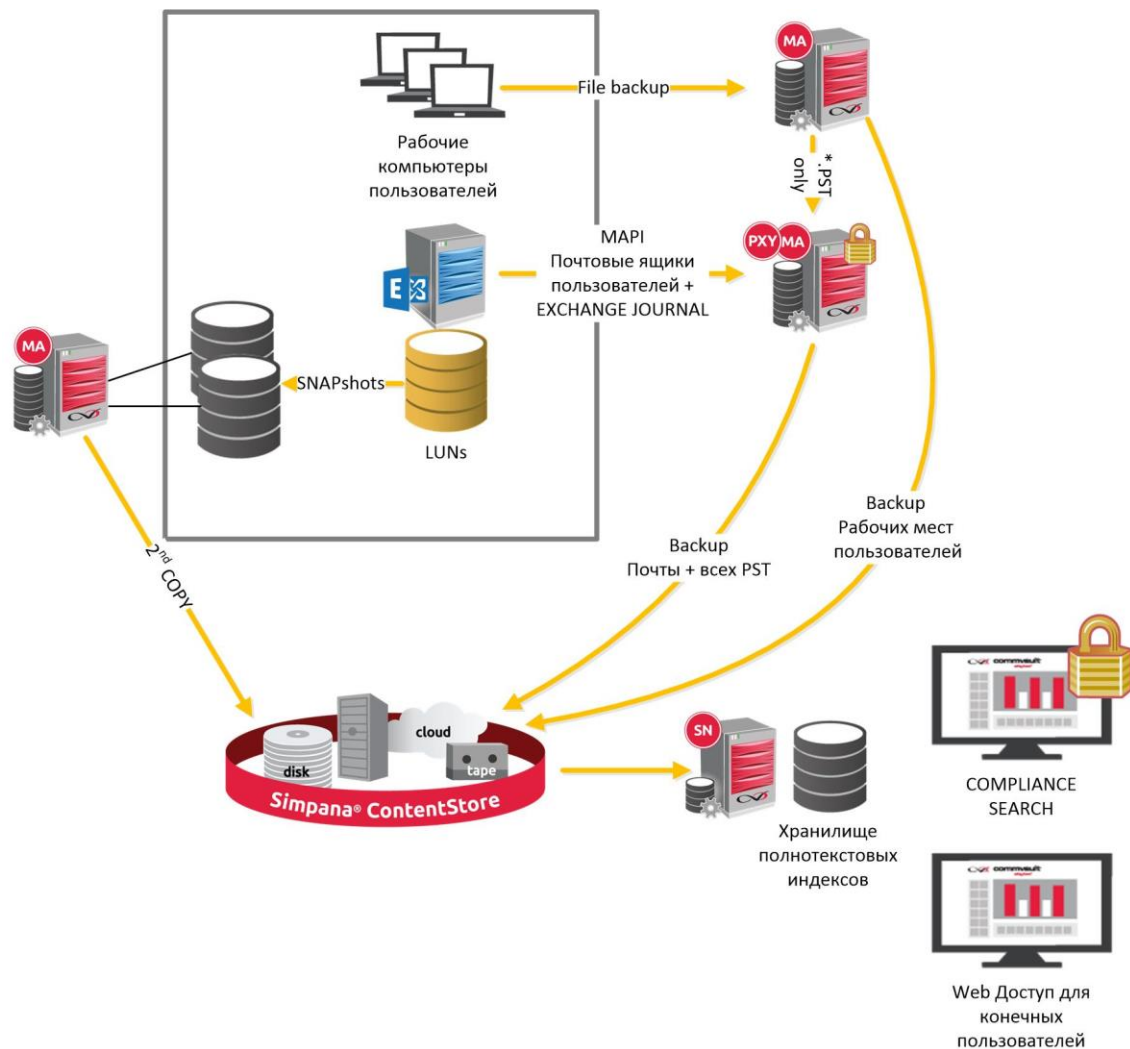
**CommCell:** [Redacted]  
**Type:** Operation - Event Viewer Events  
**Detected Criteria:** Event Viewer Events  
**Detected Time:** [Redacted] 15:29:43 2020

- Event ID: 13658036
- Monitoring Criteria: (Event Code equals to 7:211|7:212)
- Severity: Critical
- Event Date: 15:29:24 2020
- Program: CVD
- Client: ecs-p-mrweb
- Description: Detected file activity anomaly of type [Modification] minutes. Number of files Modified [55066] Deleted [6] Created [7]. Please verify the data on the machine.

Please click [here](#) for more details



# Пример решения : Защита данных + ИБ



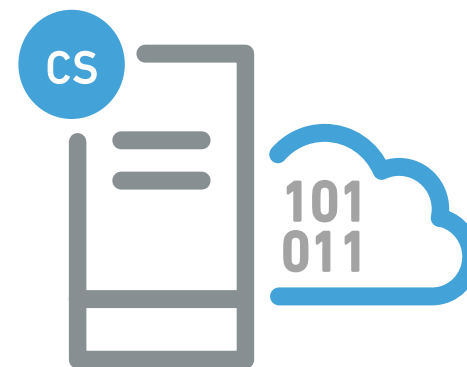
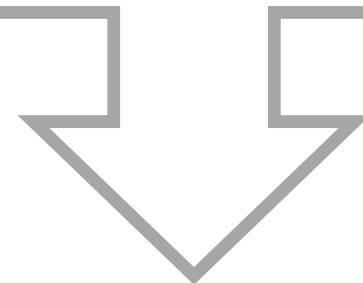
- Сбор всех документов вместе с \*.pst архивами с рабочих станций ( в том числе незаметно для пользователей)
- Сбор журнала Exchange
- Контекстное индексирование
- Анализ на предмет ненадлежащего контента, ненадлежащих адресатов и т.п.

# 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

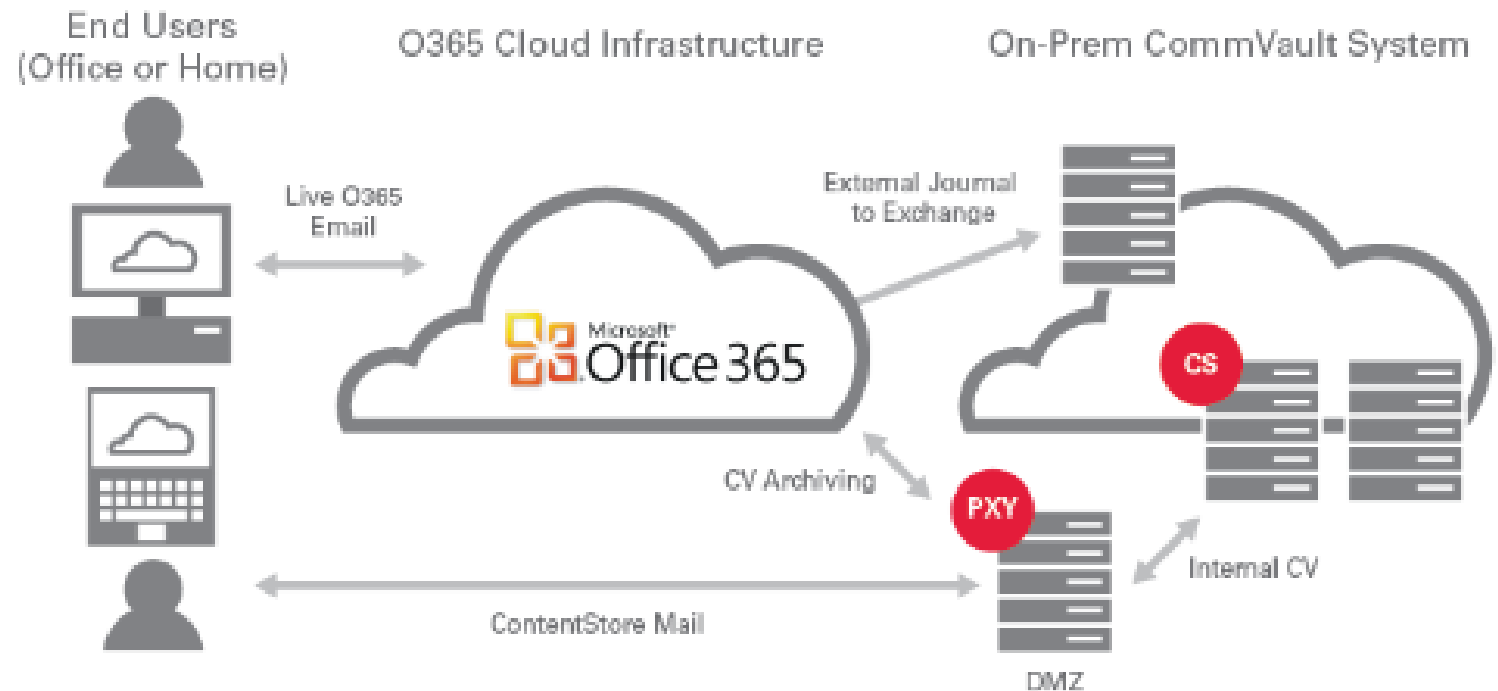
# Интеграция с Office 365. Google mail. OneDrive

## 0365 Integration

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

## Почему O365 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

The screenshot displays a user interface for managing entities. On the left, the 'Entity list' panel includes a search bar and a scrollable list of categories and items: Austria (Austria Passport), Custom Entity (Russia Passport), Danish (Danish Passport, Danish SSN), Dutch (Dutch SSN), Financial (Money, Routing transit number, Sentiment tags), and Finland. On the right, the 'Entity details' panel shows the selected entity 'Russia Passport' with the following attributes: Entity name (Russia Passport), Regular expression (empty), Derived from (None), Keywords (Passport, Russia, Russian Federation, FMS), Sensitivity (High), and Category (Custom Entity).

# Удобные панели управления

**COMMVAULT Command Center**

Search or type / for a command

Filter navigation... Discover Details

Activate / File storage .imization /

11CS

File system

Size distribution Review

FileExtension: Documents ModifiedTime: 5 Years+ AccessTime: 1 to 2 Years Clear all

198 Files 0 Folders 45.53 MB Size

Modified Time

5 Years+	45.53 MB
4 to 5 Years	16.80 MB
3 to 4 Years	46.84 MB
2 to 3 Years	11.49 MB
1 to 2 Years	4.14 MB
0 to 1 Year	0.00 KB

Access Time

5 Years+	0.00 KB
4 to 5 Years	0.00 KB
3 to 4 Years	0.00 KB
2 to 3 Years	72.50 KB
1 to 2 Years	0.00 KB
0 to 1 Year	0.00 KB

File Size

0KB to 1MB	12.49 MB
1MB to 50MB	33.04 MB
50MB to 1GB	0.00 KB
1GB to 50GB	0.00 KB
50GB to 500GB	0.00 KB

File Type

Media	1.37 MB
-------	---------

File Information

File Name	File Location	File Owner	Size	Modified
Entities.csv	/dm2perf2.dm2.commvault.com/NFSShare/AllEntities/Entities.csv	root		
SSNEmailsCreditCards.txt	/dm2perf2.dm2.commvault.com/NFSShare/TestData/SSNEmailsCreditCards.txt	root	0.12 KB	Apr 04, 2018 03:43:06 PM
Prepare.doc	/dm2perf2.dm2.commvault.com/NFSShare/PrabhuData/2003OfficeFiles/Prepare.doc	root	20.00 KB	May 27, 2010 05:53:20 PM

1,050 Total Files

1,044 Sensitive Files

3.51 MB Size

17 Owners

Sensitivity

Critical	755
High	289
Moderate	6
None	0

Files By Entity

- Date: 1.00 k (25.94%)
- undefined: 1.00 k (25.94%)
- US Social Secur...: 755 (19.49%)
- Date of Birth: 537 (13.86%)
- Dutch Social Se...: 511 (13.19%)
- Sentiment tags: 23 (0.59%)
- Greek APM: 7 (0.18%)
- Phone: 7 (0.18%)
- Danish Passport: 6 (0.15%)
- Swedish Passport...: 6 (0.15%)
- German Passport: 5 (0.13%)
- Email: 3 (0.08%)
- Hostname: 3 (0.08%)
- Canadian Social...: 1 (0.03%)

Risks

Critical	0
High	999
Moderate	45
None	0

Files By Risks

- Expired Files: 40 (1.52%)
- Retention Not Set: 999 (47.96%)
- Accessible By Everyone: (0%)
- Not Protected: 1.04 k (50.12%)

Violations By Location

World map showing India highlighted.

Sensitive Files By Department

- Development: 396 (100%)

Protected Files

- Not Protected: 1.04 k (100%)

Modified Time

0 to 1 Year	1.05 k
-------------	--------

Created Time

5 Years+	884
4 to 5 Years	48
3 to 4 Years	34
2 to 3 Years	36
1 to 2 Years	47
0 to 1 Year	1

Files By Sensitivity Score

Beyond 5K	0
1000 - 5000	0
500 - 1000	0
100 - 500	0
Below 100	1.04 k

Files By Expiration

10 - 20 Years	0
5 - 10 Years	0
1 - 5 Years	5
Not Set	999
Expired	40

7 (43.97%)

ss: 116 (18.41%)

ne: 77 (12.22%)

1 (8.1%)

ocial Secur...: 39 (6.19%)

SteuerID: 33 (5.24%)

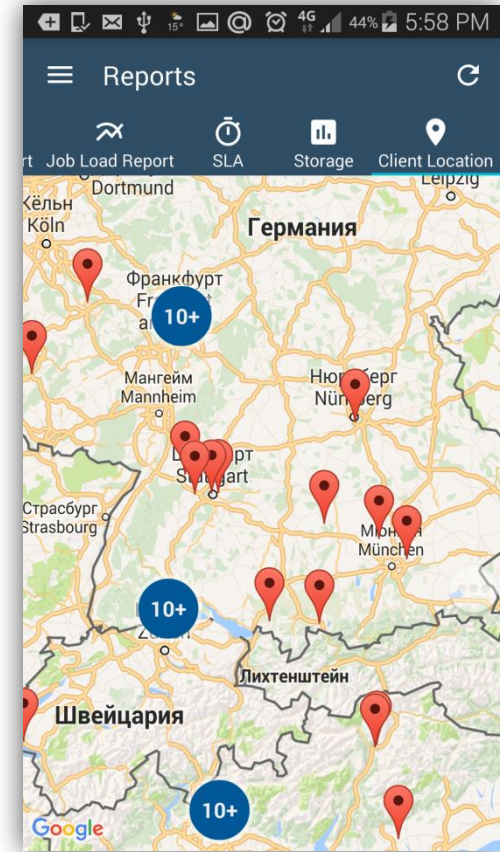
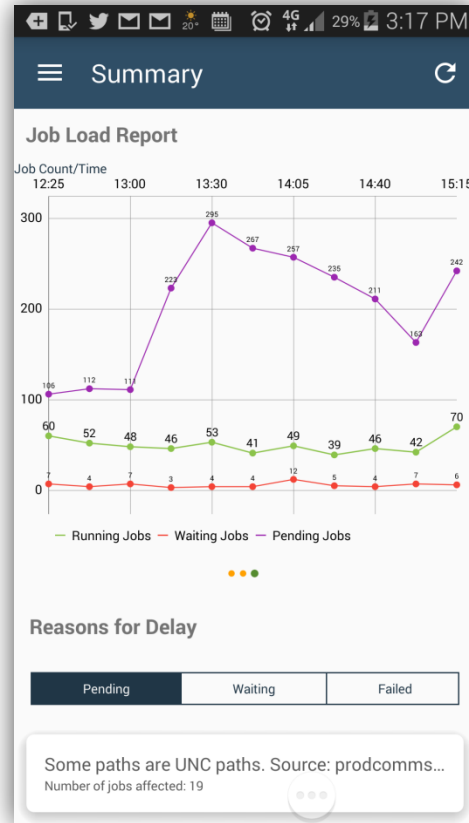
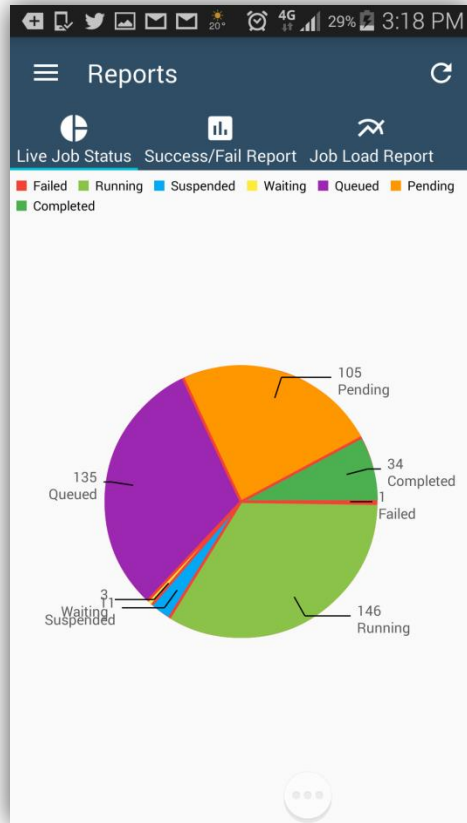
nt tags: 11 (1.75%)

1 (1.75%)

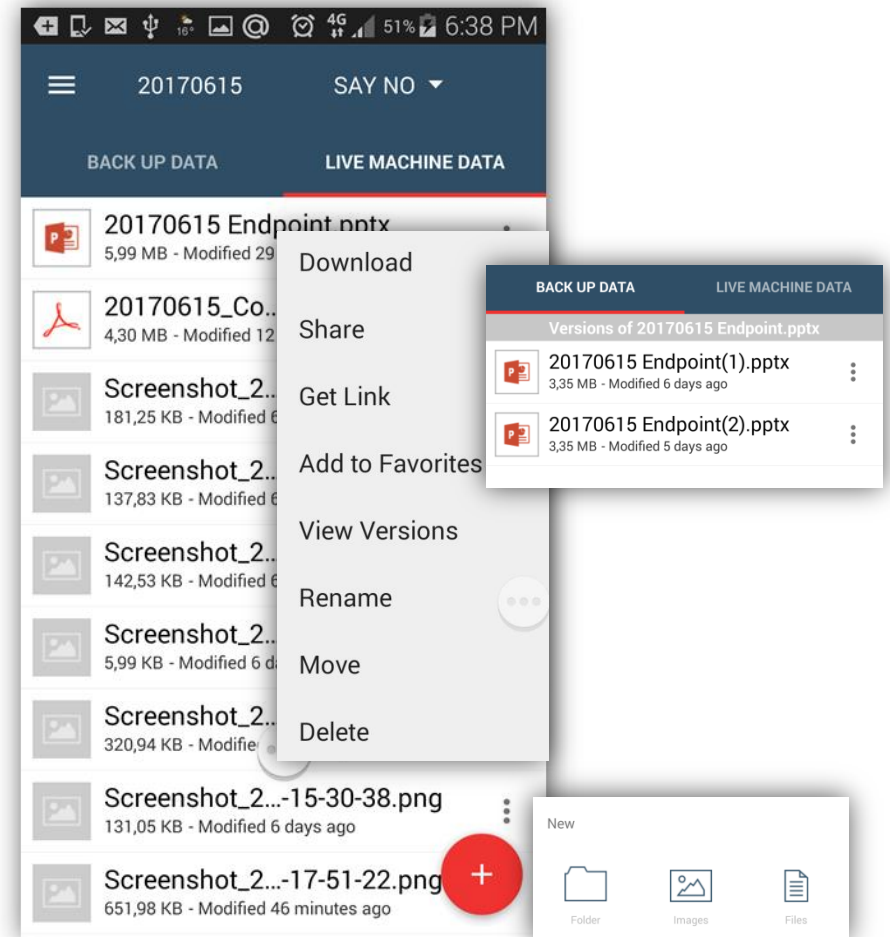
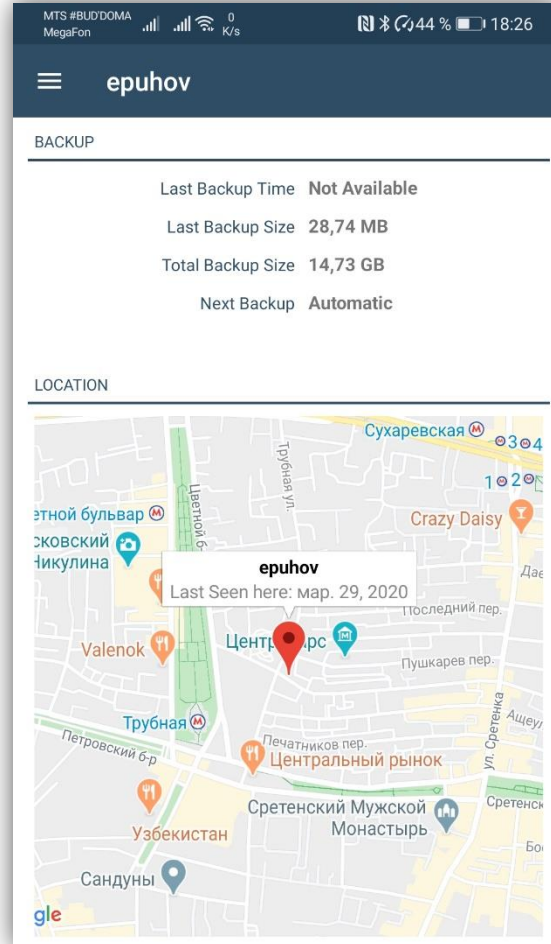
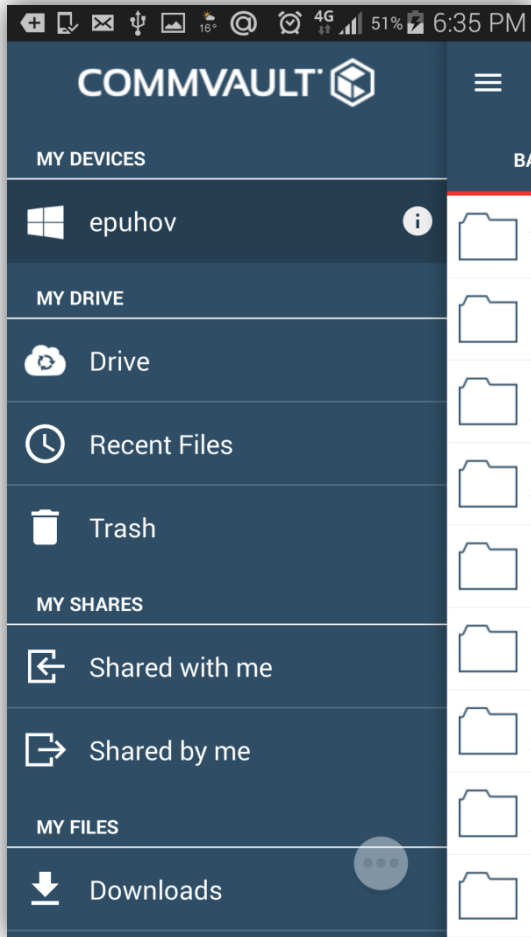
N: 10 (1.59%)

(0.79%)

# ► Мобильное приложение для мониторинга РК



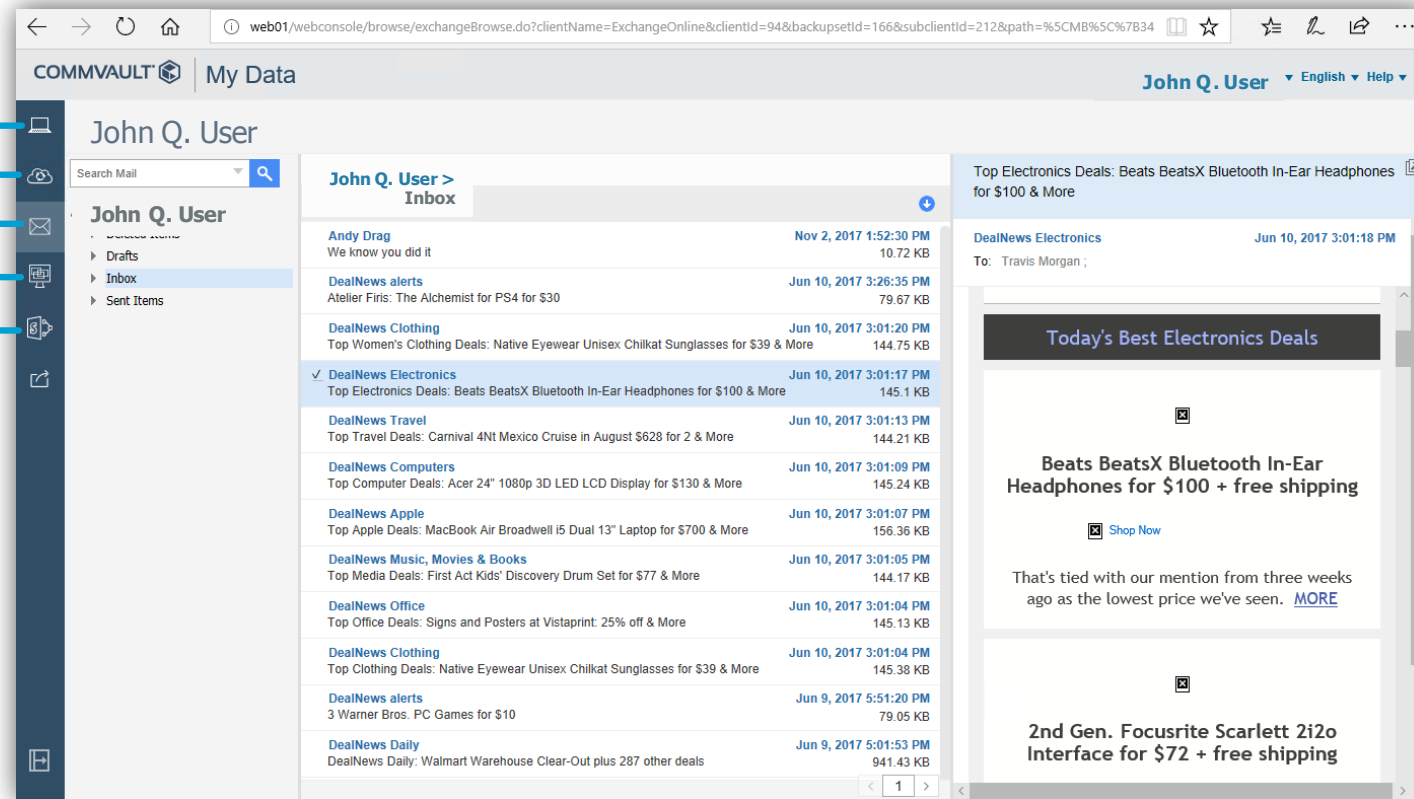
# Мобильное приложение для доступа к данным



# ► Веб Консоль конечного пользователя

## Панель самообслуживания. Поиск, загрузка, управление VM

- Laptop backup ←
- Edge Drive ←
- Email ←
- Virtual machines ←
- SharePoint ←



# ► Web интерфейс Commvault Endpoint. Резервные копии

COMMVAULT ONE | Мои данные Evgeny Puhov ▾ Русский ▾ Справка ▾

Восстановление файлов Восстановить Загрузка Стереть Общий доступ Получить общедоступную ссылку 1

Показаны последние резервные копии Показать удаленные элементы

Поиск

Обзор

Избранное

Последние документы

- technical
- Advanced infrastructure de
- archive 360
- commvault features
- dedup compress
- Exchange
- HARDWARE
- intellisnap
- Lotus
- matrix
- Microsoft
- MS SQL
- OpenSTACK KVM
- ORACLE
- questionnaire
- SAP
- v11
- VMware
- Home

ерунов > Библиотеки > Документы > technical

Имя	Дата изменения	Размер
<input checked="" type="checkbox"/> Advanced infrastructure design course	Oct 10, 2016 11:27:20 AM	6.82 МБ
<input type="checkbox"/> archive 360	Feb 12, 2015 02:05:34 PM	1.3 МБ
<input type="checkbox"/> commvault features	Apr 10, 2017 08:22:44 PM	8.59 МБ
<input type="checkbox"/> dedup compress	Jun 23, 2015 12:39:28 PM	2.37 МБ
<input type="checkbox"/> Exchange		28.89 МБ
<input type="checkbox"/> HARDWARE		266.81 КБ

Показ 1 до 22 из 22 записей

Сведения

Имя: Advanced infrastructure design course

Дата изменения: Oct 10, 2016 11:27:20 AM

Размер: 6.82 МБ

Тип: folder

Комментарии

Добавить новый комментарий

Commvault Express Edge Monitor

Last Successful Backup : 08-Jun-17 19:04:55

No Backup Running

Backup Now

Settings

Size Distribution

Category	Size (MB)
Others	15.76
Advanced infrastructure design course	6.82
commvault features	8.59
VMware	12.15
ORACLE	15.85
SAP	20.72
Exchange	28.89
intellisnap	30.82
v11	38.58
Microsoft	63.75

Последнее местоположение Отметить устройство, как утерянное

# ► Web интерфейс Commvault Endpoint. **EDGE drive**

The screenshot displays the Commvault One web interface. At the top, the user is logged in as Evgeny Puhov. The main area shows a file explorer view of a folder named "DownloadPackageLocationSP7". A table lists files and folders with columns for "Имя", "Дата изменения", and "Размер".

Имя	Дата изменения	Размер
DownloadPackageLocationSP7_WinX64	Mar 27, 2017 12:11:32 PM	18.86 КБ
linux-x8664		18.86 КБ
.oem		8 байты
Commvault.app.xml		4.46 КБ
support		18.79 КБ
version		1.63 КБ
		45.5 КБ
		71.42 КБ
		10 байты
		18.79 КБ

Two modal windows are open:

- Общий доступ**: A dialog for sharing the folder. It shows the folder name "DownloadPackageLocationSP7" and allows inviting users. The user "Evgeny Puhov" is listed as the owner. A dropdown menu shows options: "Возможный просмотр" (selected) and "Можно редактировать".
- Ссылка на общий ресурс**: A dialog for generating a share link. It shows the URL: `https://drive.commvault.com/webconsole/gtll.do?gid=PkyxyBloG`. It includes options for "When does it expire?" (Never, 7 days) and "Who can access?" (Anyone with the link, users with passwords).

At the bottom right, a Windows File Explorer window shows the local "Edge Drive" view, displaying the same folder structure as the web interface.

# ► Web интерфейс Commvault Endpoint. Почта

The screenshot displays the Commvault One web interface for user Evgeny Puhov. The main content area shows an email inbox with several messages from 'TRAINING CENTER'. A dialog box is open over the inbox, titled 'Opening Download\_1497370884928.zip'. The dialog provides information about the file: 'Download\_1497370884928.zip' which is a 'Compressed (zipped) Folder (729 KB)' from 'https://drive.commvault.com'. It asks 'What should Firefox do with this file?' and offers two options: 'Open with' (selected) and 'Save File'. The 'Open with' option is set to 'Windows Explorer (default)'. There is also a checkbox for 'Do this automatically for files like this from now on.' and 'OK' and 'Cancel' buttons at the bottom.

COMMVAULT ONE | My Data

Evgeny Puhov

Search Mails

Evgeny Puhov > Inbox > subscriptions

Sort by: Date

From	Subject	Date	Size
Новости	TRAINING CENTER - Спецвыпуск, 2017 г	Jun 8, 2017 10:01:12 AM	129.16 KB
Новости	TRAINING CENTER 03, 2017	Mar 30, 2017 7:31:06 AM	
Новости	TRAINING CENTER 01, 2017		
Новости	TRAINING CENTER 7, 2016		
Новости	TRAINING CENTER №6, 2016		
Новости	TRAINING CENTER №5, 2016		
Дмитрий Пухову Евгению XIX ежегодная конференция ""ИТ-Б...			
Дмитрий Пухову Евгению XIX ежегодная конференция ""ИТ-Б...			
Дмитрий Пухову Евгению XIX ежегодная конференция ""ИТ-БИЗНЕС в МАШИНОСТРОЕНИИ, МЕТАЛЛУРГИИ, ТЭК...		May 16, 2016 4:27:00 AM	20 KB
Дмитрий		May 13, 2016 10:00:31 AM	

Новости

TRAINING CENTER

To: Evgeny Puhov;

**Уважаемые ИТ-Спе**  
Предлагаем Вашему учебному центру "Ми

**В этом выпуске:**

1. Новое направ. Ближайшие курс
2. VM-Премьера
3. VM -премьера Ближайшие авт
4. Линейка курсо ver
- Ближайшие авт
6. Ближайшие ку безопасности
7. Ближайшие ав



# Информационная безопасность. Метод Commvault

Резервное копирование при правильной реализации –  
**100%** гарантия сохранности данных

- Разделение ролей : **администратор ИБ – Data Protection Officer** ( мониторинг содержимого и активности) , **администратор ПК** ( копирование и восстановление данных и приложений)
- Защита хранилища ПК 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



Спасибо за внимание!