Акронис Инфозащита

Акронис DLP Защита

Предотвращение утечек данных в условиях удалённой работы

Полнофункциональная пробная версия

https://www.devicelock.com/ru/download/

Удалённый доступ к работе с данными

Типы оконечных устройств и подключений

Устройства

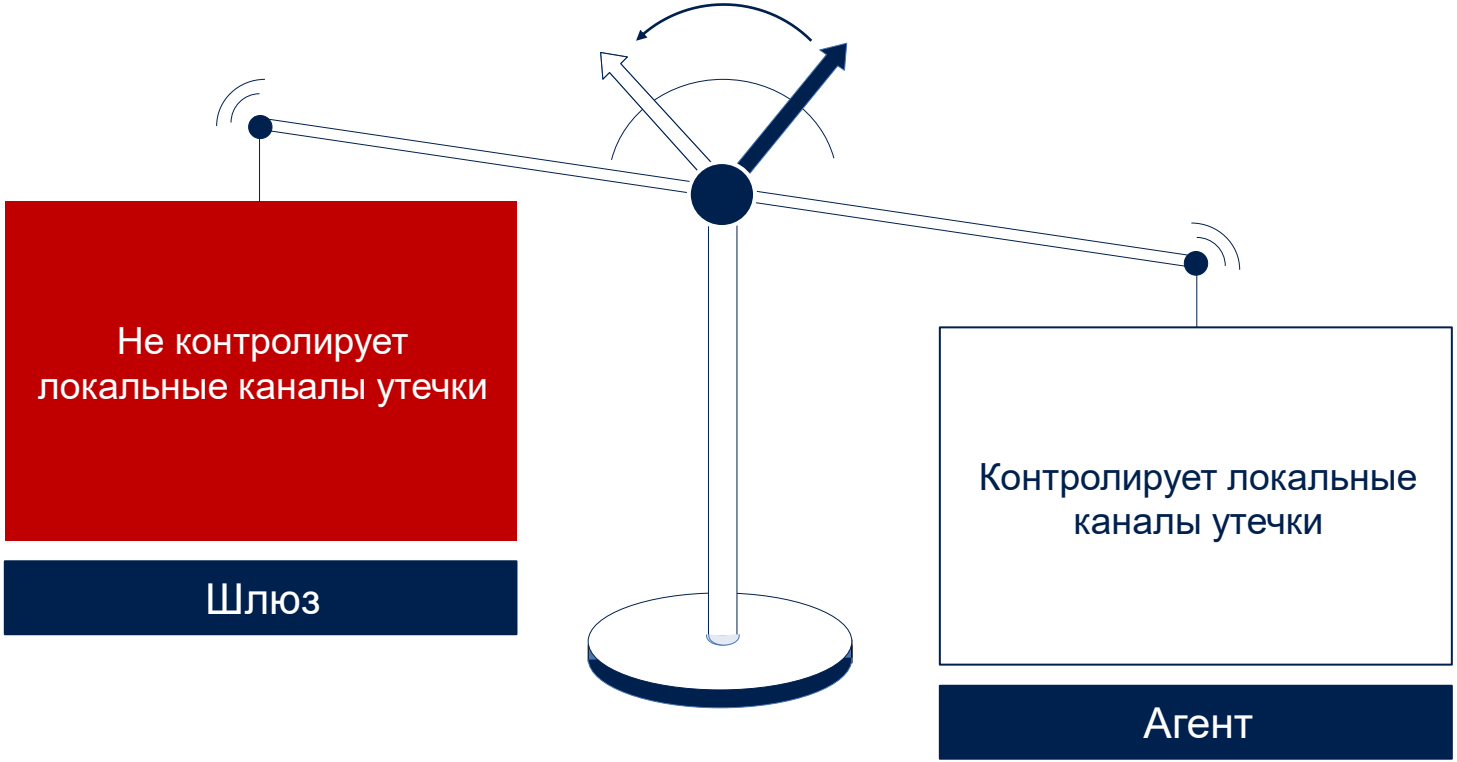
Личные	Корпоративные
Нерешаемые технические и юридические **препятствия** к установке защитного программного обеспечения	**Решаемые** технические и **отсутствующие** юридические **препятствия** к установке защитного программного обеспечения
Нулевая стоимость владения и обслуживания	**Высокая стоимость** владения и обслуживания

Подключения

VPN	RDP
Прямое подключение к корпоративным ресурсам (порталам, серверам, хранилищам)	**Подключение** к физическим / виртуальным **рабочим местам** или виртуализированным **приложениям**

Сеть предприятия

Техническая реализация предотвращения утечек



Особенности терминальных сред

Потенциальные каналы утечки

Встроенные средства контроля

Неизбирательность контроля

Полная блокировка перенаправления устройств и использования буфера обмена влияет на бизнес-процессы

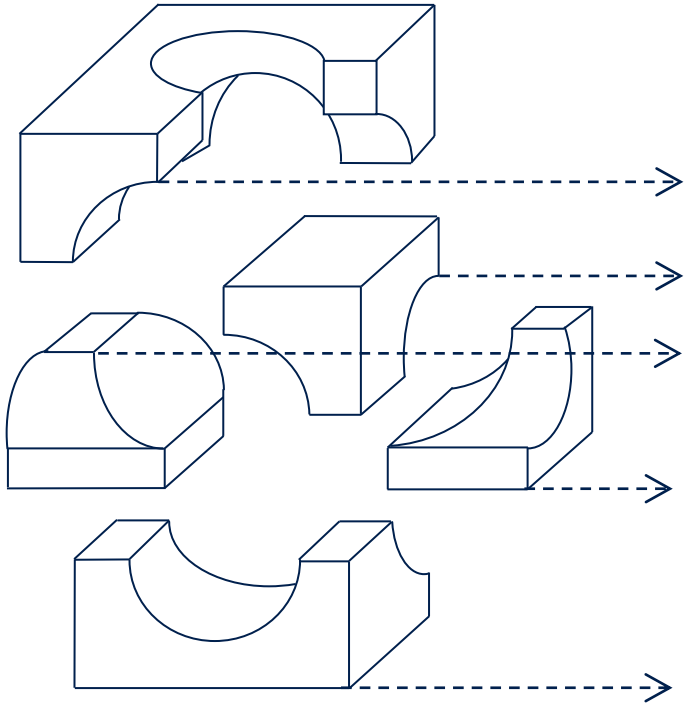
Ограниченность применения

Не контролируется содержимое буфера обмена и данных, попадающих на перенаправленные устройства

Отсутствие возможности контроля сетевых коммуникаций

Выводы

Относительно оптимальной реализации защиты от утечек данных



Масштабируемое DLP

Терминальный доступ к работе с данными

Виртуализированные рабочие столы / приложения

Хостовое DLP для полноценного контроля

Агент DLP на терминальном сервере

Технология Virtual DLP

Контролируемые каналы утечки

Буфер обмена

Распознавание типов данных: файл, текст, изображения, аудио

Перенаправленные устройства

Подключённые съёмные, жесткие, диски, оптический привод, последовательный порт, принтеры

Сетевые коммуникации

Производятся и **контролируются на терминальном сервере**

Особенности контроля

Контекстный и контентный контроль

Контроль вне зависимости от пользовательской ОС без установки дополнительных приложений

Отдельные политики DLP для каждого пользователя

Предотвращение утечек данных с мобильных устройств

Варианты реализации в моделях BYOD (GYOD/CYOD)

Агенты для мобильных устройств

- Разнообразие мобильных ОС
- **Root-доступ** на ОС Android
- **Юридические** / организационные **препятствия** к установке на личные устройства
- **Слабая аппаратная часть** не позволяет реализовать полноценный контентный контроль

Сетевой трафик через сервер DLP

- Легкое переключение на внешнюю (мобильную) сеть
- **Все минусы сетевых решений**
- Отсутствие контроля используемых данных, «закрытых» протоколов

Может использоваться как компонент решения DLP в отдельных сценариях

Решения класса EMM/MDM

- Минусы агентов для мобильных устройств
- Могут работать без подключения к сети

Могут использоваться как компоненты решений DLP в ряде сценариев

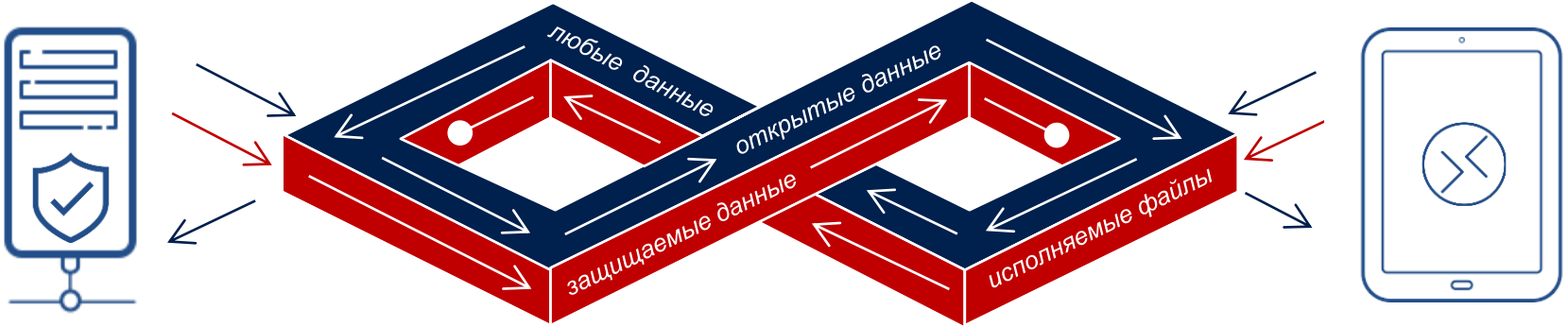
Virtual DLP

Ключевой недостаток – неудобство работы с десктопами / десктопными приложениями с экранов мобильных устройств

Полноценное DLP в реальном времени

Пример: контроль буфера обмена

В зависимости от направления передачи и содержимого данных



Терминальный сервер с агентом Акронис DLP Защита

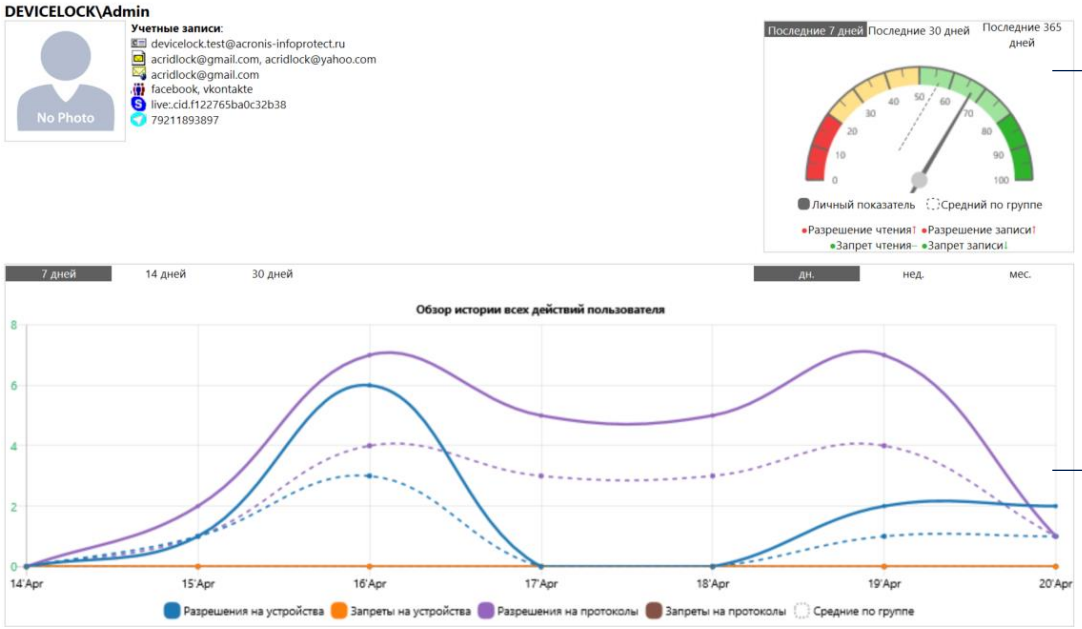
Терминальный клиент

Использование остальных каналов (дисков, портов, устройств) – запрещено полностью

Сетевые коммуникации и их контроль осуществляются непосредственно на сервере

Работа с рисками в Акронис DLP Защита

Превентивное выявление девиантного поведения



Досье (карточка пользователя)

Поведенческий анализ

Индикатор отклонения от нормы

- **Визуальное представление сравнения среднего** уровня активности за отчетный период **с базовым уровнем** (норма)
- Позволяет выявить изменения в поведении пользователя и **определить, действует ли он типично** (показатель ближе к 100%) **или аномально** (показатель ближе к 0%)

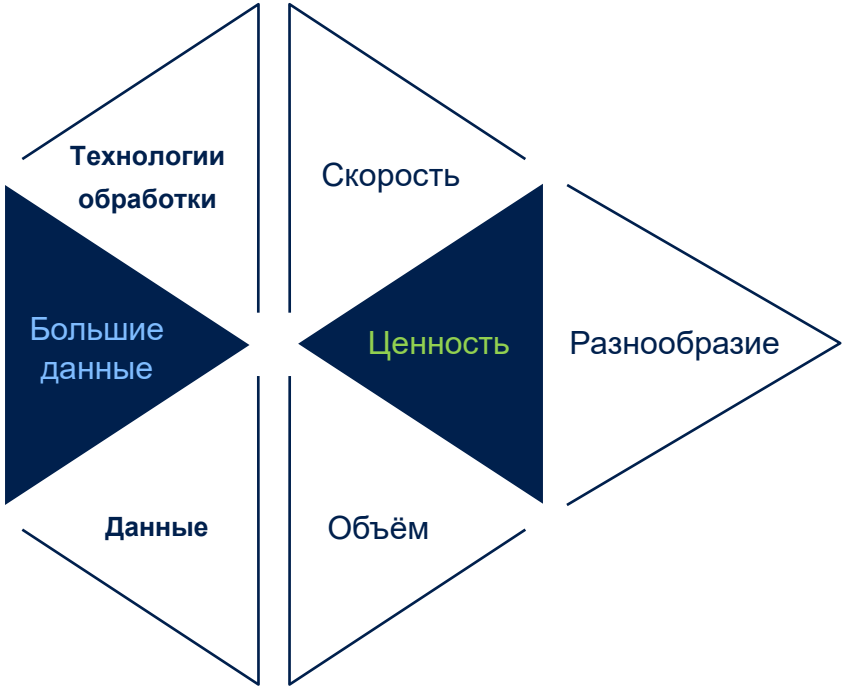
Статистический анализ

Обзор действий пользователя

- Визуальное представление активности: **разрешенные и запрещенные операции**
- **Сравнение** со средними значениями **по группе**

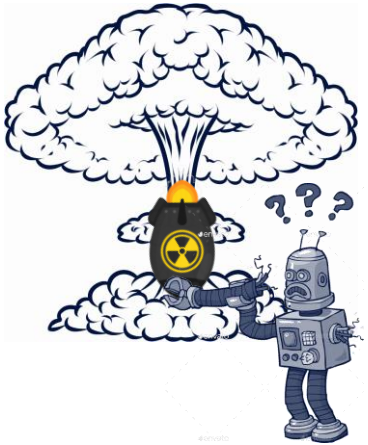
Современное DLP нежизнеспособно без данных

Ценность которых тем выше, чем их больше



- Технологии обработки обязаны своим существованием предмету обработки
- Качество анализа прямо зависит от объёма исходных данных

Базис обеспечения работы с данными – их хранение и защита



Защита данных от потери и утечки

Задача, которую необходимо решать комплексно

Акронис DLP Защита

Программный комплекс **предотвращения утечек** данных

Акронис Защита Данных

Резервное копирование систем любой сложности
с защитой от вирусов-шифровальщиков и оценкой уязвимостей

Акронис Инфозащита

Продукты и решения

Акронис
Защита Данных

Резервное копирование ИТ-систем любой сложности с централизованным управлением и оптимизацией хранения

Акронис
Защита Данных Облачная

Резервное копирование данных в физических, виртуальных и облачных средах **для поставщиков услуг**

Акронис
Инфраструктура

Масштабируемое, экономичное и универсальное п**рограммно-определяемое решение:** виртуализация, хранилище и сеть

Акронис
DLP Защита

Программный комплекс **предотвращения утечек** данных

Часть экосистемы программного обеспечения отечественных разработчиков с постоянно расширяющейся **сетью технологических партнёрств**

Единый реестр российского ПО, сертификация ФСТЭК

Акронис Инфозащита

Благодарю за внимание

Вопросы?

Тимур Гусейнов

timur.guseynov@acronis-infoprotect.ru