Acronis

DLP в условиях удаленной работы

DeviceLock Virtual DLP

Сергей Вахонин

16 декабря 2020 г.

Dual headquarters
in Switzerland and Singapore

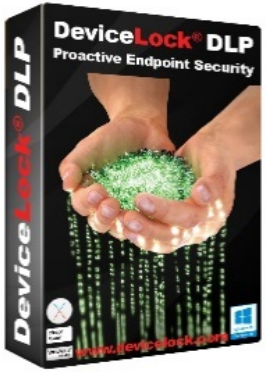
Защита информации при удаленной работе сотрудников

Сергей Вахонин

Head of DLP Support

Acronis

DeviceLock Virtual DLP



ПЕРВАЯ ВЕРСИЯ DEVICELOCK -

1996

Программный комплекс

DeviceLock® DLP

Система защиты информации для организаций, которым необходимо простое и доступное решение по предотвращению утечек данных с корпоративных компьютеров под управлением Windows и MacOS, а также виртуализованных рабочих сред и приложений Windows. Обеспечивает защиту 4 млн компьютеров в более чем 5 тыс. организаций по всему миру.

DeviceLock®

AN ACRONIS COMPANY

В июле 2020 DeviceLock стал частью компании Acronis.

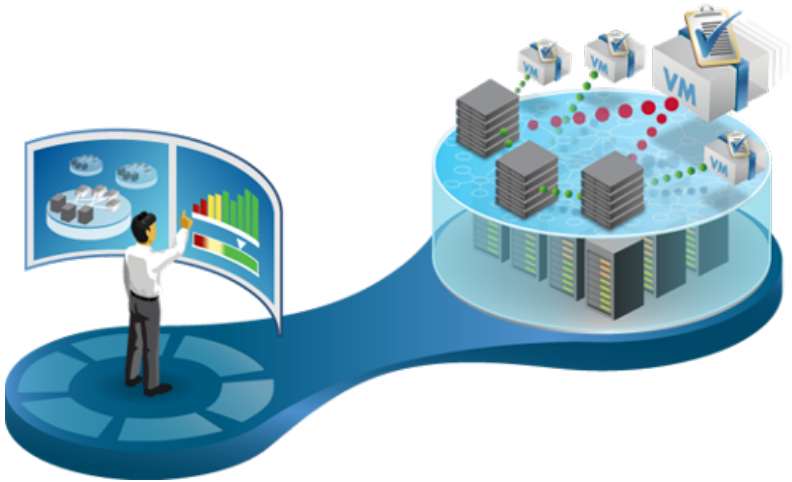
В 2021 г. планируется выпуск новой версии Acronis DeviceLock DLP 9 и интеграция DLP-технологий DeviceLock в Acronis Cyber Protect.

Acronis

Удаленная работа - удаленный доступ

Использование сред виртуализации и удаленного доступа в корпоративных ИТ для обеспечения удаленной работы

Преимущества сред виртуализации



- Повышение изоляции и общей безопасности, ограничение доступа к данным
- Распределение ресурсов (дисковых ресурсов, памяти, сетевого трафика)
- **Стерильная рабочая среда**, созданная исключительно для выполнения бизнес-задач
- **Универсальный доступ к десктопам, приложениям и данным - разнообразие операционных систем и аппаратных платформ для доступа к виртуализованной среде**

Работа в виртуализованных средах

Доступ к конфиденциальной информации - через терминальные серверы

Виртуальные десктопы в VDI

Десктопы в терминальной сессии

Виртуализованные приложения

RDP,
ICA,
PCoIP,
HTML5

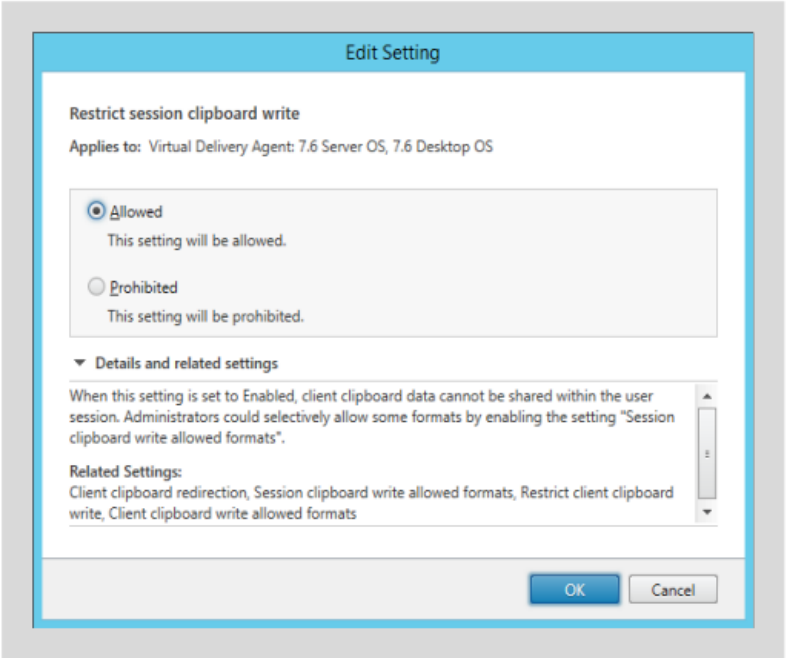
Терминальный клиент

Использование технического решения на основе терминального сервера позволяет обеспечить защиту от несанкционированного копирования конфиденциальной информации на внешние носители за счёт того, что вся информация хранится не на рабочих станциях, а на терминальном сервере.

Безопасность данных в средах виртуализации

Ограниченность встроенных средств

- Встроенные средства в решениях для создания виртуальных сред позволяют создать конфигурацию, когда полностью блокируются перенаправление локальных устройств и ограничивается использование буфера обмена, что может нарушить нормальные бизнес-процессы пользователя.
- **Содержимое** буфера обмена и данных, попадающих на перенаправленные устройства, никак не контролируется средами виртуализации.
- Сетевые коммуникации (мессенджеры, почта, облака, ...), доступные и используемые **внутри** виртуального рабочего стола (или в качестве виртуального приложения) также не контролируются решениями по удаленной виртуализации с точки зрения защиты от утечки конфиденциальных данных.



Acronis

Сценарии удаленной работы

Типовые варианты и риски их использования

Удаленный режим работы: типовые сценарии

В корпоративную сеть – через VPN

Используется служебный или личный компьютер с прямым доступом к корпоративным ресурсам

В корпоративную сеть – через RDP к рабочему месту

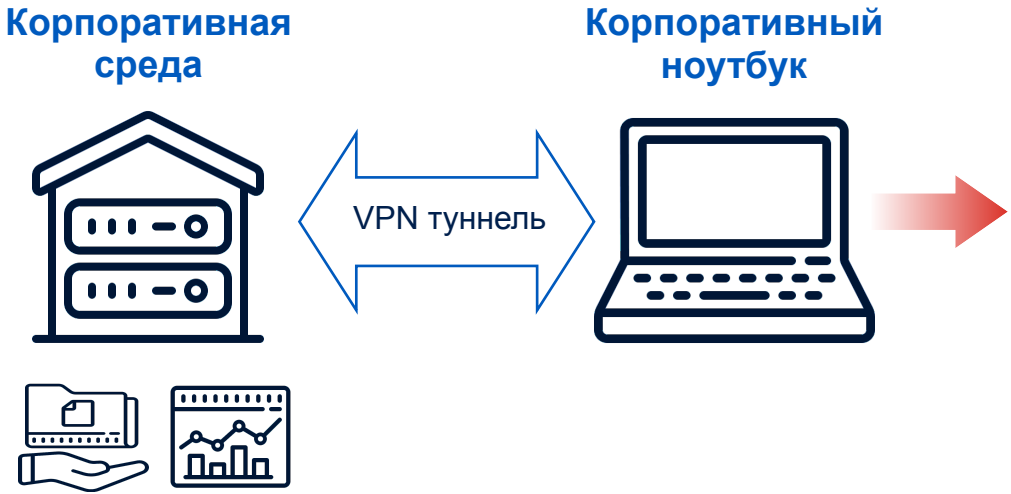
Рабочий компьютер функционирует в офисе, для доступа используется RDP

В корпоративную сеть – через терминальный сервер

Подключение к терминальному серверу с любого устройства

В корпоративную сеть – через VPN

Использование корпоративного устройства с прямым подключением к корпоративным ресурсам (порталам, серверам, хранилищам) через VPN



Без DLP-агента на ноутбуке:
Высокий риск утечки и дальнейшего бесконтрольного распространения сохраненных **локально** данных при отключении от VPN

Использование периферийных устройств (накопителей, принтеров)

Неконтролируемые сетевые коммуникации (почта, мессенджеры, облачные хранилища, …)

Удаленный доступ (RDP) к рабочему месту

Использование личного/служебного устройства с RDP-подключением к рабочему месту в офисе

Рабочее место (удаленный ПК)

Личный ПК

RDP сессия

Копирование файлов с рабочего ПК и доступных с него сетевых ресурсов на личное устройство через **буфер обмена** в терминальной сессии, **перенаправленные устройства**

Невозможность установки DLP-решения на личный компьютер: Высокий риск утечки и дальнейшего бесконтрольного распространения данных

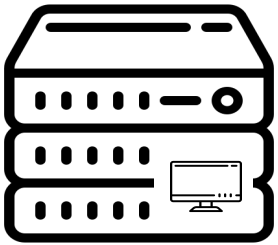
Использование периферийных устройств (накопителей, принтеров)

Неконтролируемые сетевые коммуникации (почта, мессенджеры, облачные хранилища, …)

Удаленный доступ к терминальному серверу

Использование личного/служебного устройства с RDP-подключением к виртуальным рабочим местам / виртуализованным приложениям

Удаленный рабочий стол



RDP сессия

Личный ПК

Копирование файлов из корпоративной среды на личное устройство через **буфер обмена** в терминальной сессии, **перенаправленные устройства**

Невозможность установки DLP-решения на личный компьютер: Высокий риск утечки и дальнейшего бесконтрольного распространения данных

Использование периферийных устройств (накопителей, принтеров)

Неконтролируемые сетевые коммуникации (почта, мессенджеры, облачные хранилища, …)

Удаленный режим работы: типовые решения

Базовые подходы к защите информации при удаленном режиме работы

В корпоративную сеть – через VPN

- Использование полнофункционального DLP-агента на корпоративном компьютере

RDP к рабочему месту

- Использование полнофункционального DLP-агента на корпоративном компьютере (рабочем месте)
- DLP-защита для RDP-подключения

Виртуализованные рабочие места

- DLP-защита для терминальных сессий

Acronis

DLP-защита в виртуальной среде

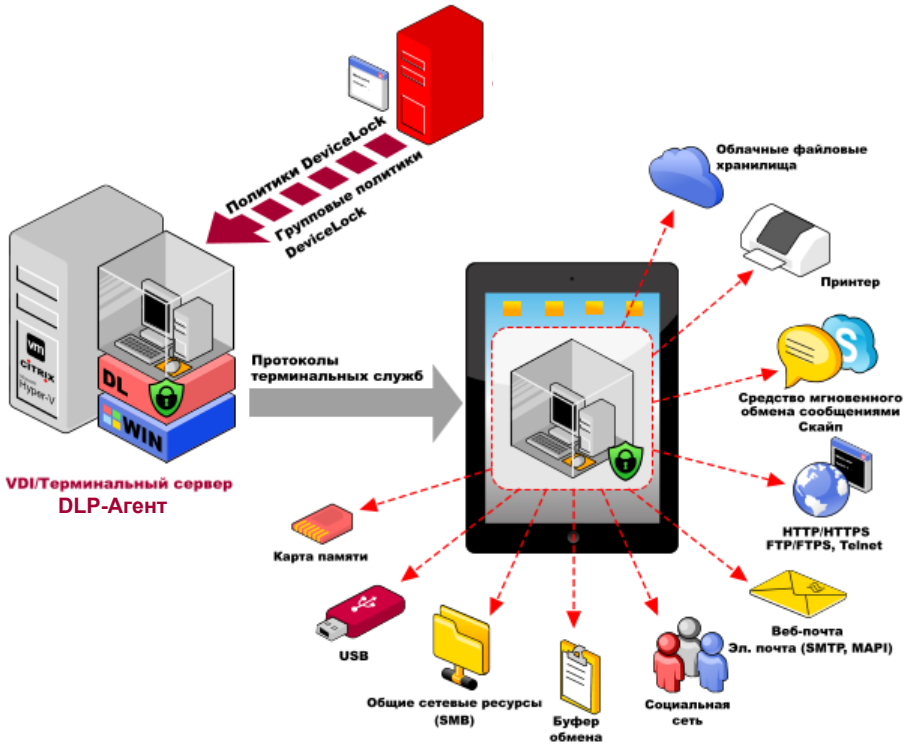
Защита от утечки данных в терминальных сессиях

DLP-защита данных в виртуальной среде

Технология DeviceLock Virtual DLP

DLP-агент функционирует внутри терминальной сессии

- Использование виртуальной рабочей среды вместо локального контейнера
- Отсутствие зависимости от операционной системы на клиенте:
  применимость на любых персональных устройствах (планшеты, лэптопы, тонкие клиенты, домашние компьютеры с любыми операционными системами).
- DLP-агент функционирует внутри терминальной сессии (в виртуальной среде)



Контролируемый удаленный доступ к данным

DLP-агент функционирует внутри терминальной сессии

- Приложения, опубликованные на гипервизорах (XenApp)
- Локальные виртуальные машины
- Терминальные сессии рабочих столов, в т.ч. опубликованных на гипервизорах
- Решения для виртуализации от Microsoft (RDS/RDP), Citrix (XenApp, XenDesktop) и VMware (VMware View)
- Детектирование перенаправленных устройств в сессии независимо от используемых протоколов (Microsoft RDP/ RemoteFX, Citrix ICA/HDX)

Защита данных для удалённых рабочих мест

Контролируемые каналы утечки

Буфер обмена в терминальной сессии

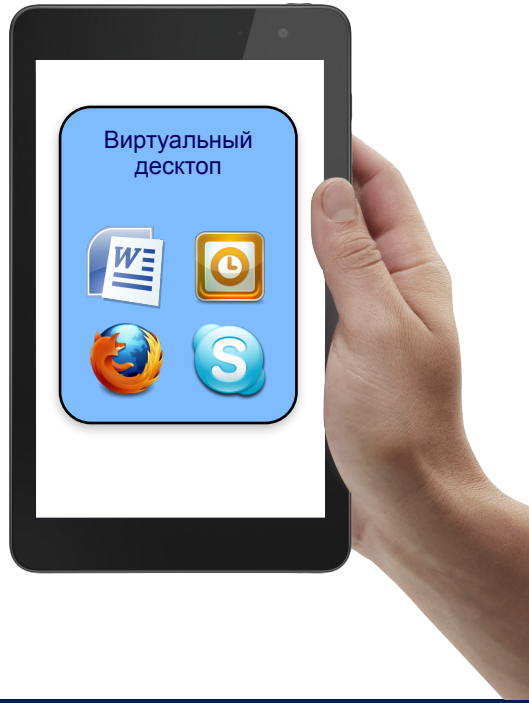
Распознавание типов данных: файл, текст, изображения, аудио

Перенаправленные устройства

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

Сетевые коммуникации

Устанавливаются и **контролируются на терминальном сервере**



Особенности контроля

Контекстный контроль каналов передачи данных в сочетании или независимо от контентной фильтрации в режиме реального времени

Контроль вне зависимости от ОС удаленного терминала без установки дополнительных приложений

Индивидуальные политики DLP для отдельных пользователей или групп

Полноценный DLP-контроль

Контроль доступа + фильтрация содержимого передаваемых данных

Разрешение передачи данных
нет нарушения политики защиты данных ограниченного доступа – передача разрешена

Точная копия переданных данных, журналирование событий
(как при блокировке, так и по факту разрешенной передачи данных)

Тревожное оповещение

Блокировка передачи данных
При попытке использования запрещенных каналов передачи данных или нарушения политики защиты данных ограниченного доступа

Запись экрана и клавиатурного ввода
по заданным событиям

Преимущества анализа в реальном времени

DeviceLock Virtual DLP

Предотвращение утечки данных

Нет бесконтрольного распространения данных

- Блокировка передачи данных при детектировании данных ограниченного доступа
- Гибкий контроль доступа к буферу обмена данными и устройствам, перенаправленным в терминальную сессию

Нет помех для бизнес-процессов

Отсутствие блокировки передачи данных, если нет защищаемых данных

- Данные передаются после **анализа содержимого** с запретом передачи только данных ограниченного доступа
- Отсутствие зависимости от операционной системы на клиенте

Оперативная реакция ИБ

Тревожные оповещения по заданным событиям

- Немедленное выявление инцидента в форме **попытки** запрещенной передачи данных, а не факта утечки
- Оперативное выявление злоумышленников без ущерба для организации

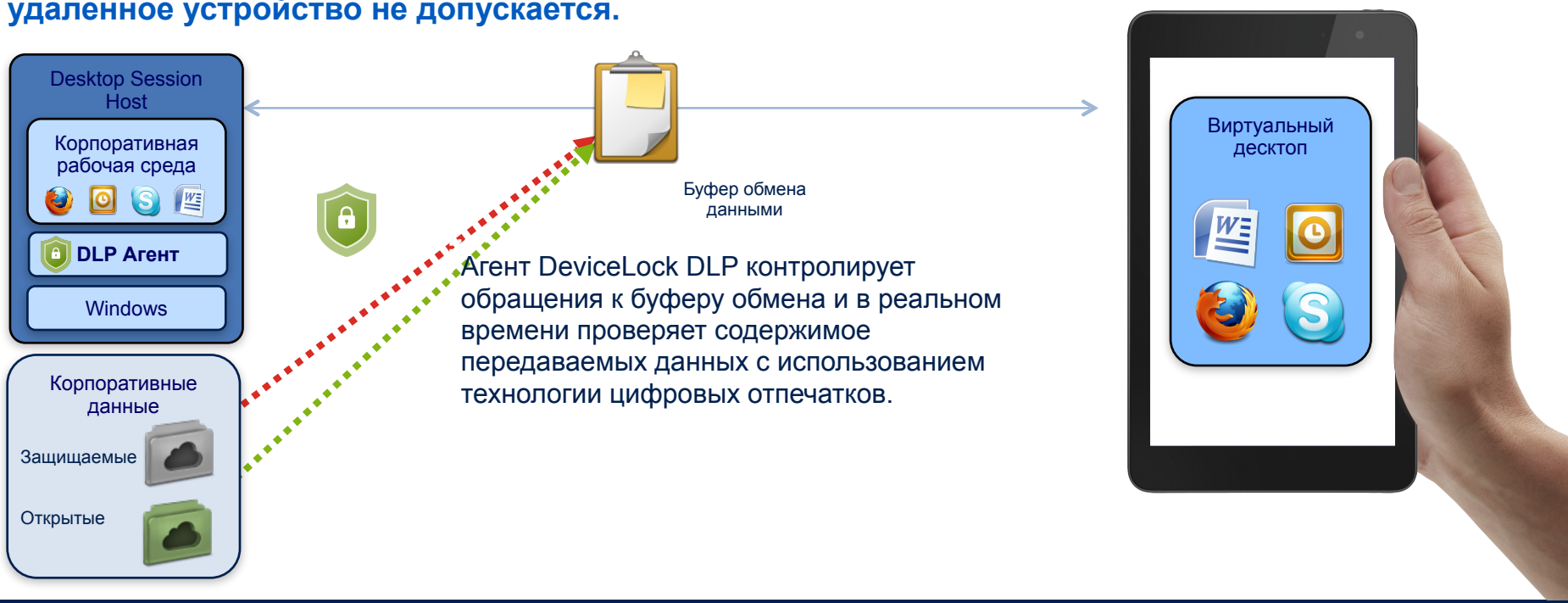
Проведение расследований

Сбор и хранение доказательной базы

- Точная копия переданных данных создается (как при блокировке, так и по факту разрешенной передачи данных)
- Запись экрана по заданным событиям

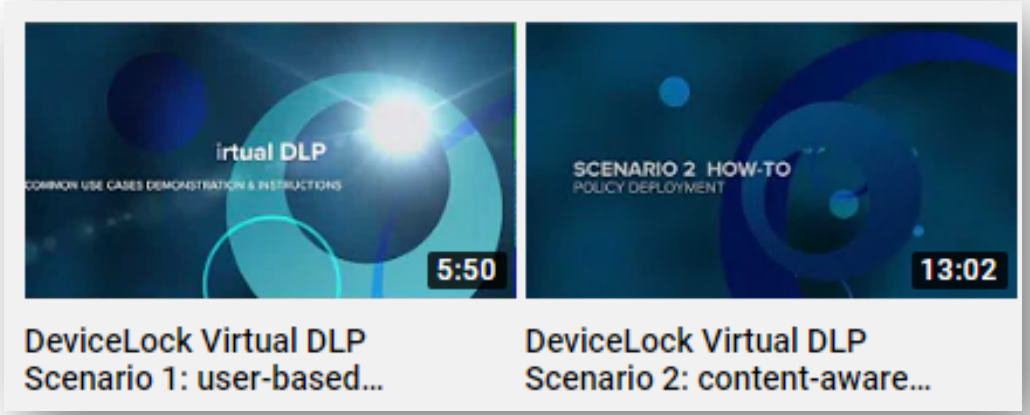
Пример реализации DeviceLock Virtual DLP

Работа с конфиденциальными данными выполняется в корпоративной рабочей среде на сервере через терминальную сессию к опубликованному рабочему столу. Неавторизованная передача данных из хранилища конфиденциальных документов на удаленное устройство не допускается.



Как защититься от утечки?

Помощь для организаций, перешедших на удаленный режим



https://www.youtube.com/user/DeviceLockVideo/videos

По запросу – краткая инструкция по установке и настройке DeviceLock DLP в комплекте с типовыми конфигурационными файлами

DeviceLock®

AN ACRONIS COMPANY

Спасибо!