DeviceLock DLP
Proactive Endpoint Security

ЗАЩИТА КОРПОРАТИВНЫХ ДАННЫХ В ВИРТУАЛЬНОЙ СРЕДЕ

ТЕХНОЛОГИЯ DEVICELOCK VIRTUAL DLP

СЕРГЕЙ ВАХОНИН

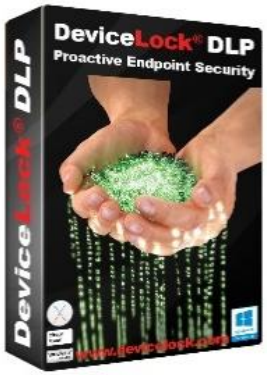
Директор по решениям

Смарт Лайн Инк / DeviceLock, Inc.

EMAIL SV@DEVICELOCK.COM

АО Смарт Лайн Инк
Москва, 09/2018

АО «Смарт Лайн Инк» - 20 лет на рынке информационной безопасности



ПЕРВАЯ ВЕРСИЯ
DEVICELOCK -
1996

Продукт

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.

Смарт Лайн Инк / DeviceLock, Inc.

Отечественная компания с штаб-квартирой и офисом разработки **в Москве** (АО «Смарт Лайн Инк),
офисами продаж в США (DeviceLock NA, San Ramon, California), Канаде (DeviceLock Canada, North Vancouver), Великобритании (DeviceLock UK, London), Германии (DeviceLock Europe GmbH, Ratingen), Италии (DeviceLock Italy, Milan),
а также партнерской сетью по всему миру.

Более 70 000 пользователей при более чем 7 000 000 инсталляций по всему миру

DeviceLock - 20 лет на рынке информационной безопасности всего мира

DeviceLock DLP – настоящее DLP для защиты информации

DeviceLock DLP

ПРЕДОТВРАЩЕНИЕ УТЕЧЕК ДАННЫХ и МОНИТОРИНГ СОБЫТИЙ

в режиме реального времени, в любых сценариях!

…устройства и интерфейсы

…каналы сетевых коммуникаций

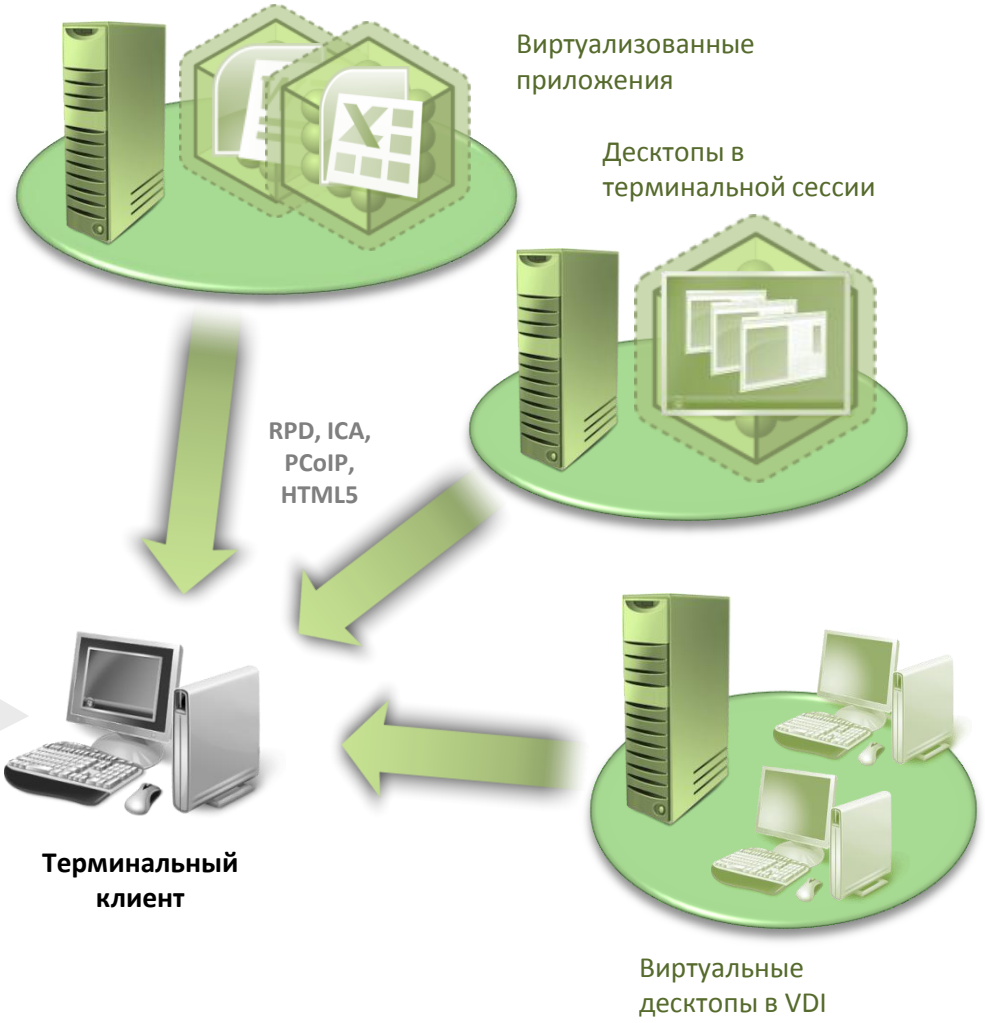
…с применением технологий контентной фильтрации

+ собственный поисковый сервер

+ сканирование хранимых данных

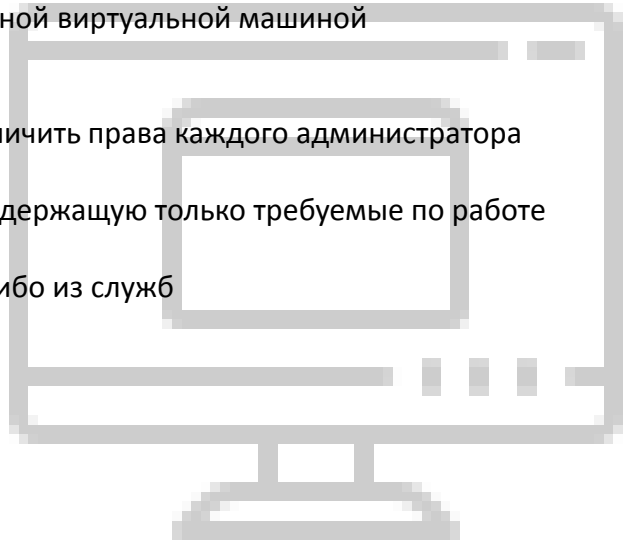
Технология
DeviceLock VirtualDLP

Среды виртуализации и удаленного доступа в корпоративных ИТ



Преимущества сред виртуализации

- **Повышение изоляции**
  - Ограничение одной или группы тесно связанных служб собственной виртуальной машиной
  - Снижение вероятности сбоев от взаимного влияния программ
- **Безопасность**
  - Распределение задач администрирования — возможность ограничить права каждого администратора только самыми необходимыми
  - Ограничение доступа к данным – возможность создать среду, содержащую только требуемые по работе приложения
  - Снижение потенциальных вредных последствий взлома какой-либо из служб
- **Распределение ресурсов**
  - Выделение памяти по требованию
  - Гибкое распределение сетевого трафика между машинами
  - Распределение дисковых ресурсов
- **Постоянная доступность и повышение качества администрирования**
  - Возможность live-миграции машин
  - Плавный апгрейд критических серверов
- **Универсальный доступ к десктопам, приложениям и данным - разнообразие операционных систем и аппаратных платформ для доступа к виртуализованной среде.**



Стерильная рабочая среда, созданной ИТ-подразделением исключительно для выполнения бизнес-задач сотрудников, является, пожалуй, самым идеальным вариантом со многих точек зрения. Такая среда содержит те и только те бизнес-инструменты, которые необходимы пользователю для его задач – от полноценной windows-среды в форме виртуальной машины (рабочего стола) до отдельного опубликованного приложения, например, в среде Citrix Virtual Apps (ранее XenApp), доступ к которым пользователь получает через терминальную сессию.

Специфика обработки данных в средах виртуализации

Обработка данных.
Данные приложений и пользователей обрабатываются в рамках виртуальных машин. В рамках одного сервера может существовать множество виртуальных серверов, на каждом из которых могут обрабатываться персональные данные различных категорий, а сами серверы могут входить в разные информационные системы персональных данных.

Передача данных.
Данные передаются:

- между виртуальными машинами внутри виртуальной среды
- между виртуальной средой и внешним клиентом (терминальным клиентом)
- между виртуальной средой и внешними средами (сетевые коммуникации)

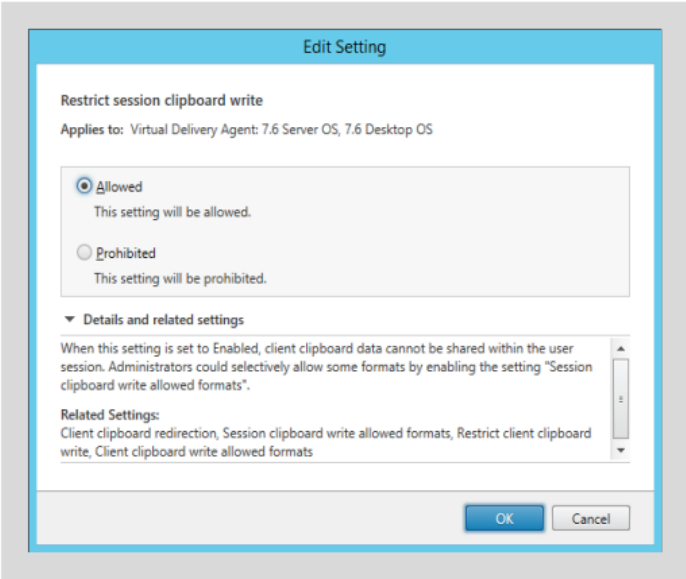
Угрозы данным в средах виртуализации.

- Угрозы аппаратной платформе
- Угрозы системному ПО виртуализации (гипервизору)
- Угрозы системе управления виртуальной средой
- Угрозы ИТ-инфраструктуре, реализованной в рамках виртуальной среды
- Угрозы сети хранения данных с размещаемыми образами виртуальных машин
- Угроза потери конфиденциальности данных при их перемещении на удаленное рабочее место или за пределы корпоративной ИС по каналам сетевых коммуникаций

Безопасность данных в средах виртуализации

Каждое из перенаправленных в терминальную сессию периферийных устройств становится неконтролируемым каналом утечки данных из сеанса виртуального рабочего стола или приложения.

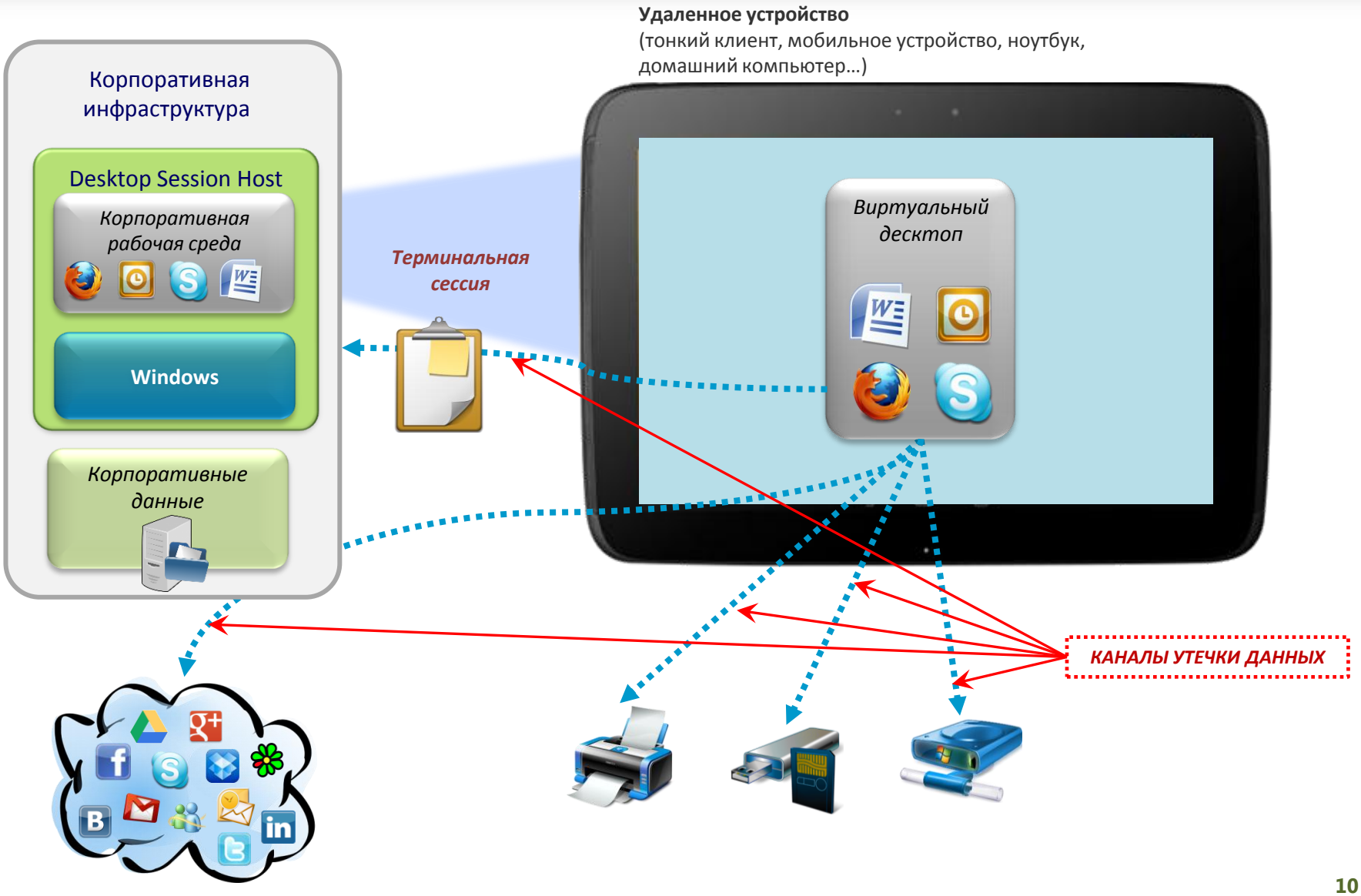
Пример 1: из бизнес-приложения на виртуальном рабочем столе пользователь может сохранить файл с корпоративными данными на флэш-накопитель, подключенный к рабочему месту, а затем «случайно» опубликовать этот файл в Интернете.
Пример 2: пользователь может распечатать конфиденциальный документ из корпоративного хранилища на домашний принтер, подключенный к личному планшету по Wi-Fi.
Пример 3: при запрете перенаправленных устройств на уровне среды виртуализации, но разрешенном буфере обмена пользователь может неконтролируемо перенести данные из буфера обмена на свой личный компьютер.



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.

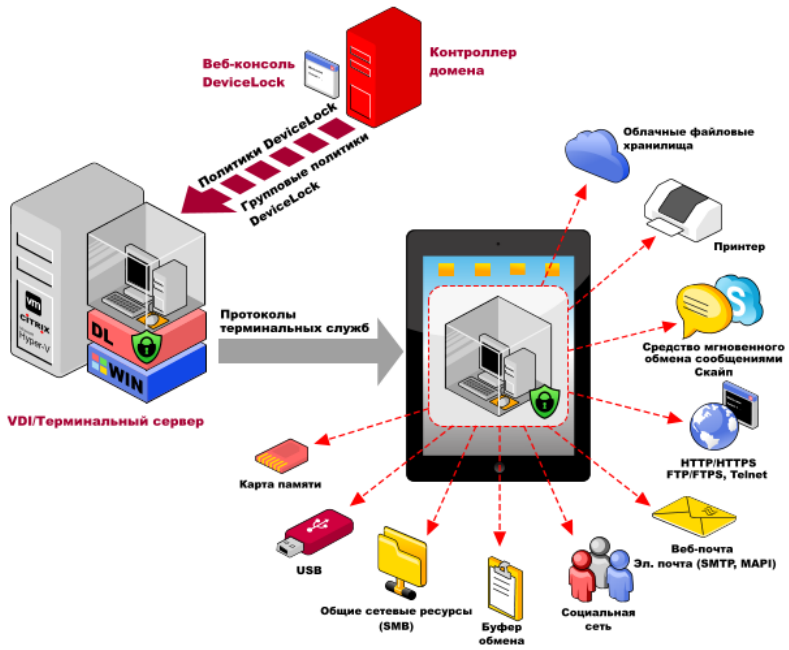
Удаленный доступ к данным в корпоративной среде



DeviceLock VirtualDLP: защита корпоративных данных в виртуальной среде

ДОСТУП К КОРПОРАТИВНЫМ ДАННЫМ – ТОЛЬКО НА ВРЕМЯ РАБОТЫ.

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

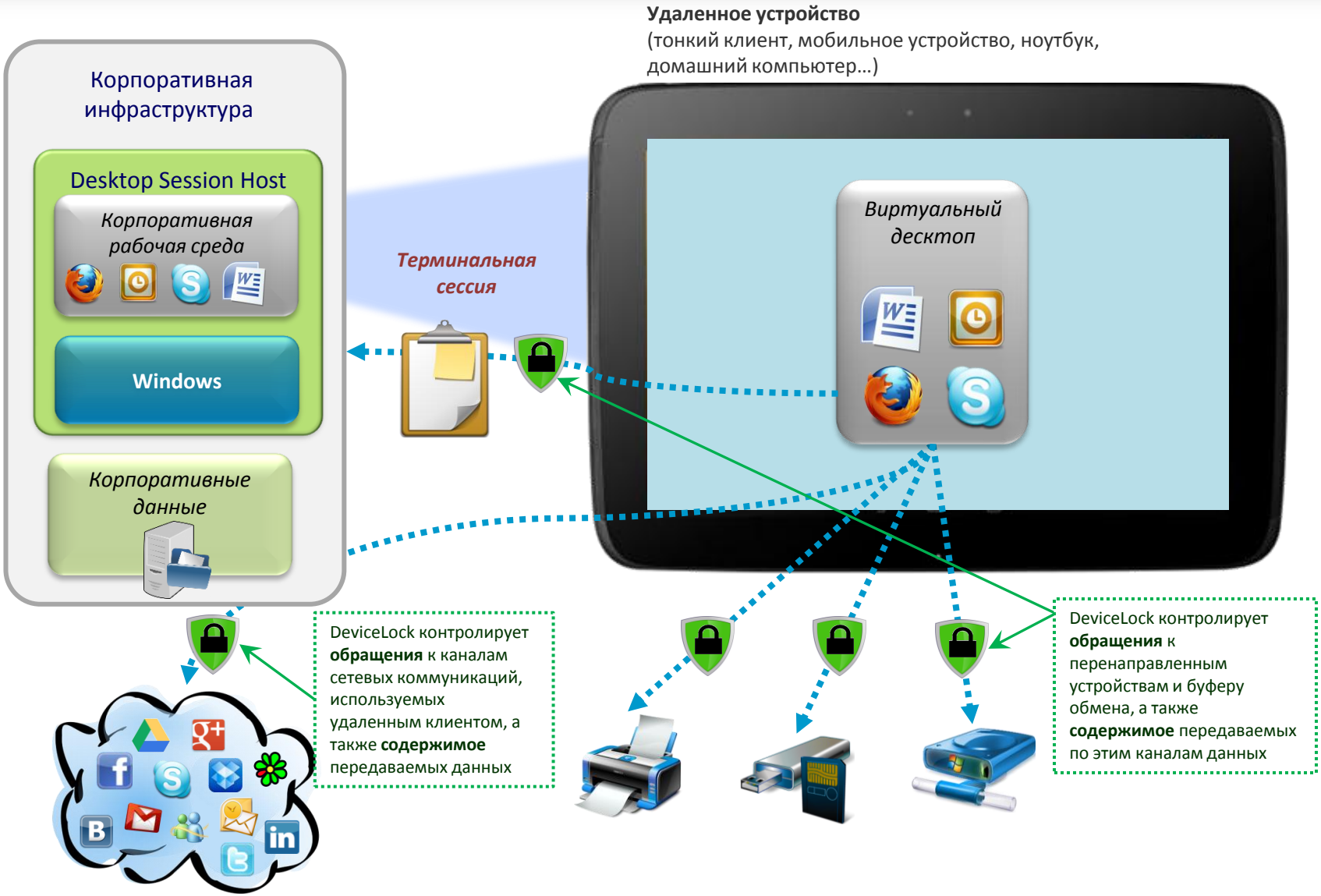


- *Приложения, опубликованные на гипервизорах (XenApp)*
- *Локальные виртуальные машины*
- *Терминальные сессии рабочих столов, в т.ч. опубликованных на гипервизорах*
- *Решения для виртуализации от Microsoft (RDS/RDP), Citrix (XenApp, XenDesktop) и VMware (VMware View)*
- *Передача данных через протоколы Microsoft RDP/RemoteFX и Citrix ICA/HDX*

vmware READY

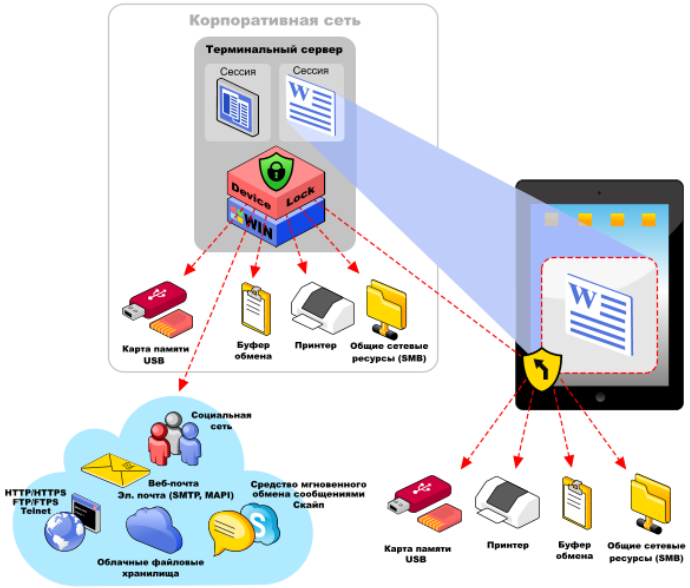
CITRIX ready

Контролируемый удаленный доступ к данным в корпоративной среде



Применение DeviceLock VirtualDLP

Технология DeviceLock Virtual DLP гарантирует, что передача данных пользователем находится строго внутри границ виртуальной терминальной среды (терминальной сессии), а данные ограниченного доступа, утечка которых недопустима, будут защищены от переноса в неконтролируемую организацией зону, оставаясь при этом доступными для эффективного выполнения бизнес-задач.



Суть **DeviceLock Virtual DLP** заключается в контроле потока данных между виртуальным рабочим столом или опубликованным приложением и перенаправленными на удаленные рабочие компьютеры периферийными устройствами, включая съемные накопители, принтеры, USB-порты и буфер обмена данными. Сетевые коммуникации пользователей внутри терминальной сессии также контролируются DLP-механизмами программного комплекса DeviceLock DLP. Также обеспечиваются централизованное журналирование действий пользователя и теневое копирование переданных им файлов и данных.

Контентная фильтрация для контроля сред виртуализации

- **Контролируемые типы содержимого:** текст, бинарные данные, типы данных
- **Методы детектирования текстового контента:** поиск по ключевым словам и словарям (160+ встроенных отраслевых терминологических словарей, возможность создания собственных словарей) с применением морфологического анализа (для английского, русского и других языков) по целым словам или частичному совпадению, с поддержкой транслитерации для русского языка; поиск по встроенным комплексным шаблонам регулярных выражений (90+ встроенных шаблонов, возможность создания собственных шаблонов); анализ по цифровым отпечаткам (с частичным или полным соответствием с заданным образцом) с поддержкой классификации образцов.
- **Методы детектирования бинарного контента**: анализ по цифровым отпечаткам
- **Контролируемые текстовые данные**: более 100 распознаваемых форматов файлов и 40+ типов архивов, текстовые данные в электронных сообщениях, веб-формах, текст в изображениях, запечатанные документы Oracle IRM, объекты данных с метками классификатора Boldon James
- **Контролируемые типы данных**: более 5300 типов файлов, свойства файлов и документов, объекты буфера обмена (файлы, текст, изображения, аудио, прочее), объекты протоколов синхронизации с мобильными устройствами, контроль текста в графических изображениях (встроенных в документы Microsoft Office, AutoCAD и Adobe PDF или отдельных графических файлах), запечатанные документы Oracle IRM, объекты данных с метками классификатора Boldon James

Демонстрация технологии

DeviceLock VirtualDLP

Некоторые сценарии

предотвращения утечки данных

в реальном времени

ИЛЬШАТ ЛАТЫПОВ

Инженер-аналитик

Смарт Лайн Инк

Сценарий: запись документа с финансовой информацией на проброшенные диски

Проброшенные диски разрешены всем.

Задача: предотвратить запись документов с конфиденциальным содержимым(ИНН) на проброшенный диск.
Все факты записи должны журналироваться, с созданием теневой копии.
При попытке записи документа с конфиденциальным содержимым следует отправлять тревожное оповещение.

Инспекция текстового содержимого (контентная фильтрация)

Создание записи в логе, теневой копии

Тревожное оповещение

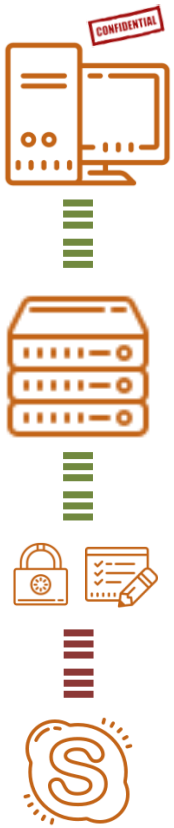
Сценарий: копирование информации через буфер обмена

Допускается копирование информации только в направлении сервера XenApp, копирование информации с сервера на тонкий клиент запрещено.

Задача: не допускать копирование информации(текста, изображения, файлов) с приложений XenApp на тонкий клиент
Создавать теневую копию переданных на сервер данных.

- Создание теневой копии
- Контроль на уровне типа передаваемых данных
- Контроль направления копирования

Сценарий: расширенный контроль Skype на XenApp



Использование Skype разрешено для всех пользователей только для передачи сообщений (чат), голосового и видео- общения.

Задача: не допускается передача документов через Skype, разрешены чат, аудио- и видео-конференции.
Уведомлять пользователя о недопустимости передачи файлов.
Вести журналирование попыток передачи файлов и содержимого чата.

- Доступ предоставляется всем пользователям и группам
- Передача документов запрещена
- Журналирование попыток передачи файлов
- Теневое копирование чата Skype
- Вывод сообщения в трее о запрете передачи файла

СПАСИБО
ЗА ВНИМАНИЕ!

www.DeviceLock.com