DeviceLock
AN ACRONIS COMPANY

Предотвращение утечек данных в условиях удалённой работы

Тимур Гусейнов

Менеджер поддержки продаж

Удалённая работа

Как частный случай повсеместной децентрализации

Государство

Делегирование полномочий муниципалитетам и коммерческим организациям

Финансы

Криптовалюты с распределённой эмиссией вместо национальных валют с центральным эмитентом

Это навсегда

Бизнес

Swarming для реализации отдельных проектов вместо постоянной иерархии

Общество

Сетевые структуры внесистемной оппозиции вместо политических партий

Удалённый доступ к работе с данными

Типы оконечных устройств и подключений

Устройства

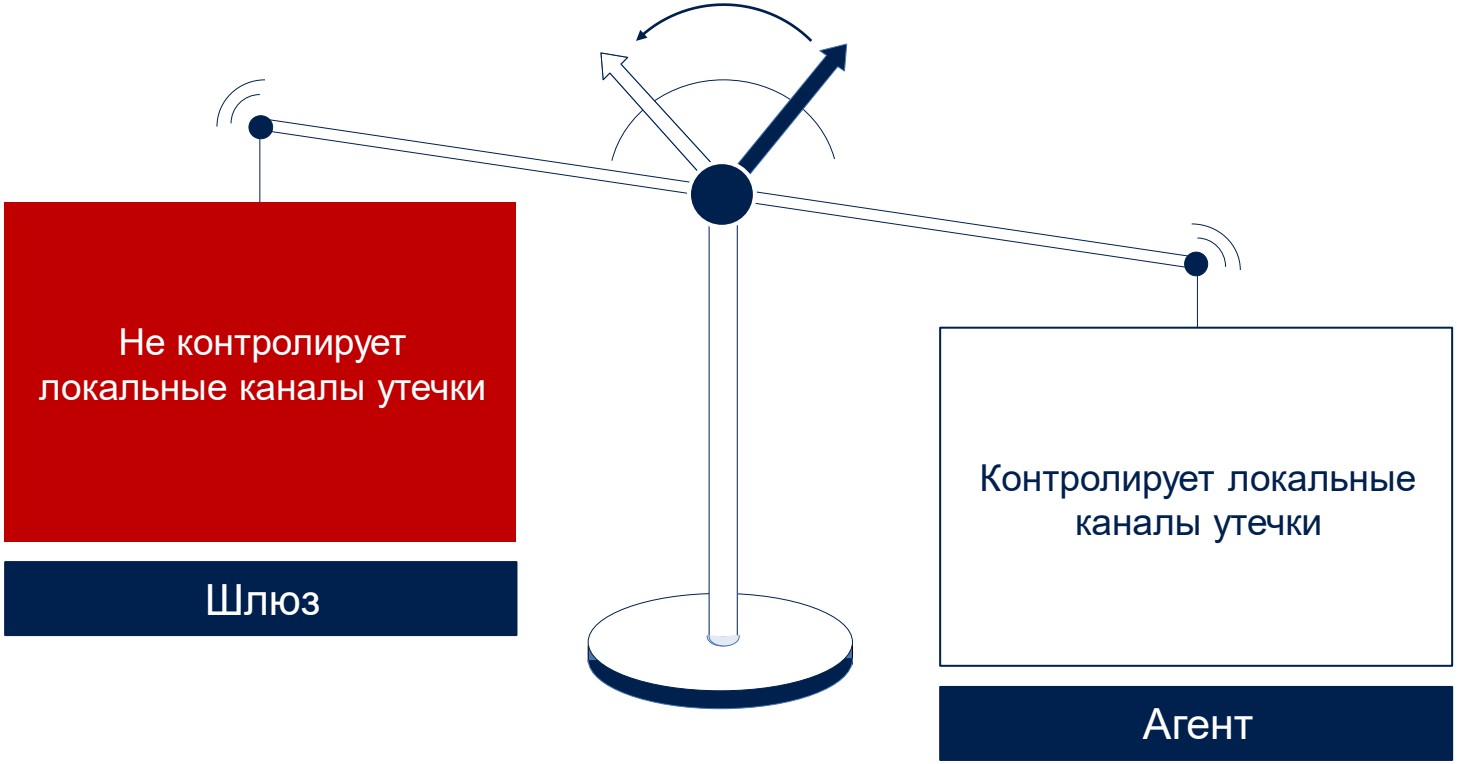
Личные	Корпоративные
Нерешаемые технические и юридические **препятствия** к установке защитного программного обеспечения	**Решаемые** технические и **отсутствующие** юридические **препятствия** к установке защитного программного обеспечения
Нулевая стоимость владения и обслуживания	**Высокая стоимость**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

Подключения

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

Корпоративная сеть

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

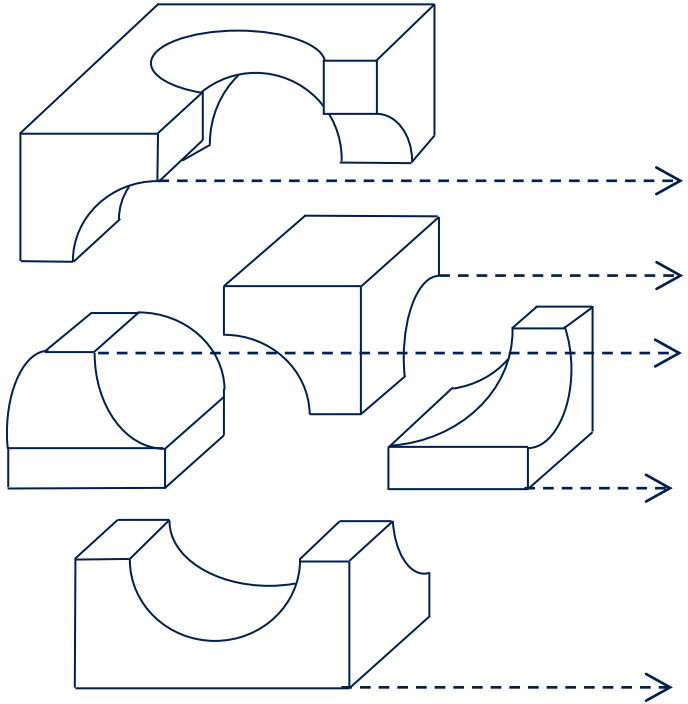
Ограниченность применения

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

Полноценное DLP в реальном времени

Технология DeviceLock 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

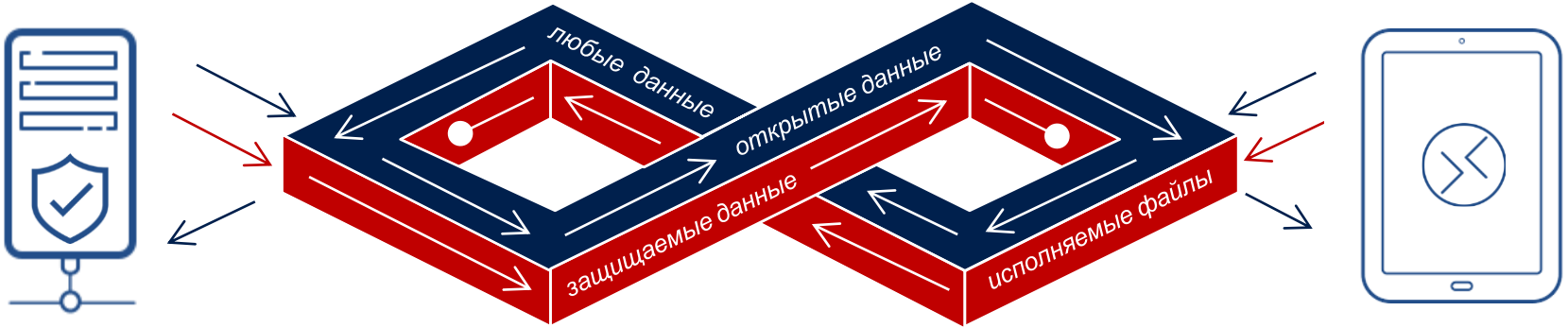
Контекстный и контентный контроль

Контроль вне зависимости от пользовательской ОС без установки дополнительных приложений

Отдельные политики DLP для каждого пользователя

Пример: контроль буфера обмена

В зависимости от направления передачи и содержимого данных



Терминальный сервер с агентом DeviceLock DLP

Терминальный клиент

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

Сетевые коммуникации и их контроль осуществляются непосредственно на сервере

Работа с контекстом инцидента

Видеозапись экрана, клавиатурного ввода, сведений о запущенных процессах

Контекст инцидента

Реализация

Гибкая настройка правил записи по двум типам триггеров и их комбинациям

Системные

Вход в систему, работа процесса, обнаружение подключений VPN, LAN, WLAN, подключение периферийных устройств

DLP

Правила контекстного и контентного контроля, использование устройств и носителей в белых списках, и т.п.

Простые правила с одним условием и сложносоставные правила

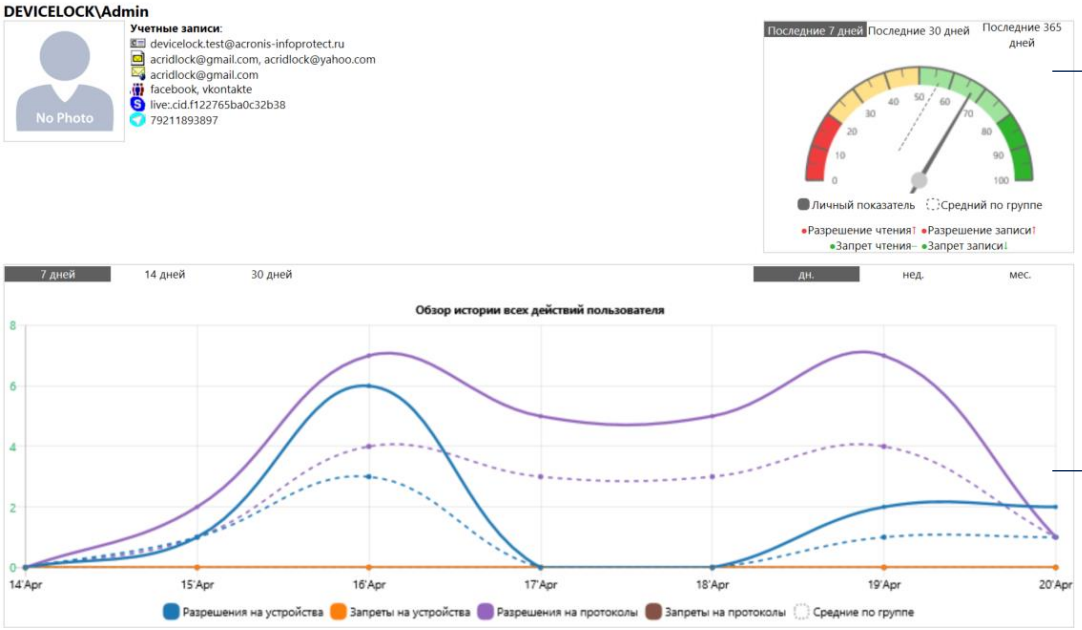
Локальное хранение записей или передача их на сервер

Цветная или ч/б запись с нескольких мониторов

Остановка записи при отсутствии активности

Стоит ли ждать инцидента?

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**

DeviceLock®
AN ACRONIS COMPANY

Благодарю за внимание

Вопросы?

Полнофункциональная пробная версия
https://www.devicelock.com/ru/download/