DeviceLock®
AN ACRONIS COMPANY

Предотвращение утечек данных

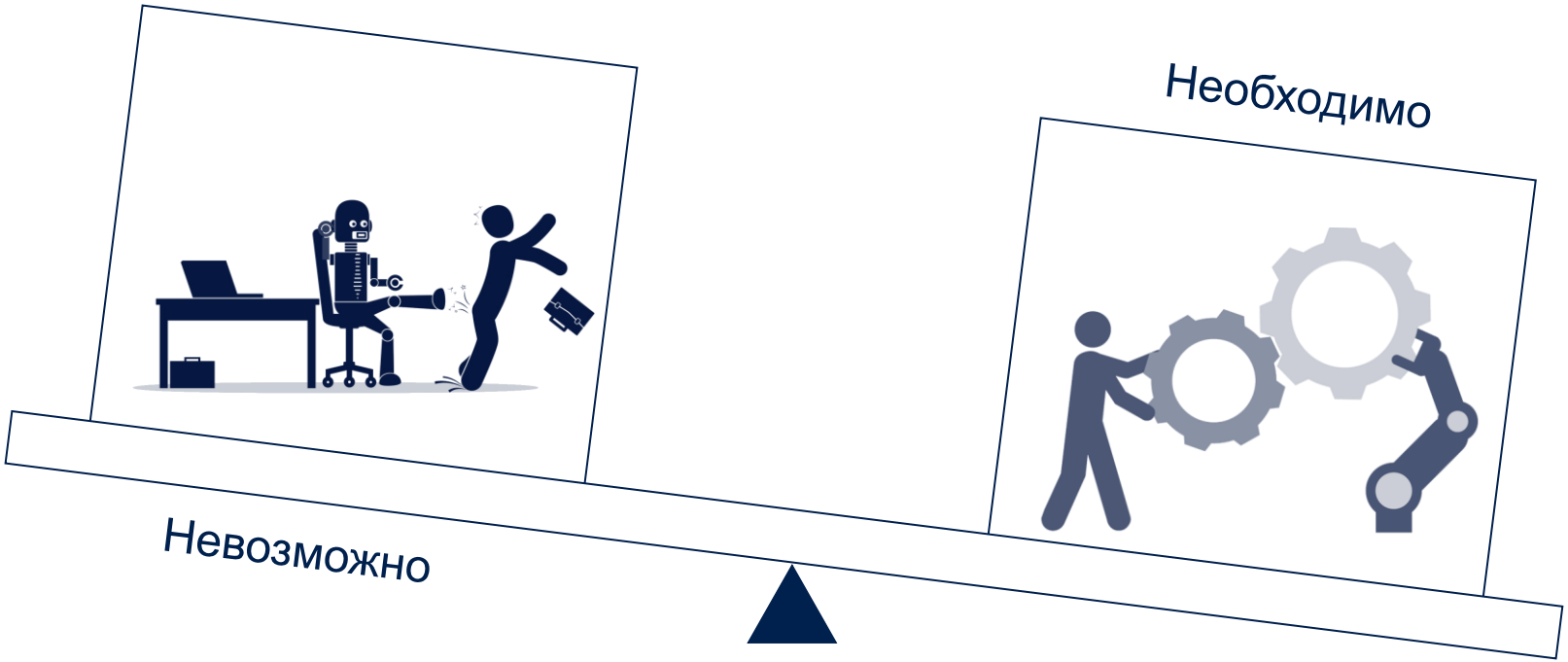
Люди и технологии

Тимур Гусейнов

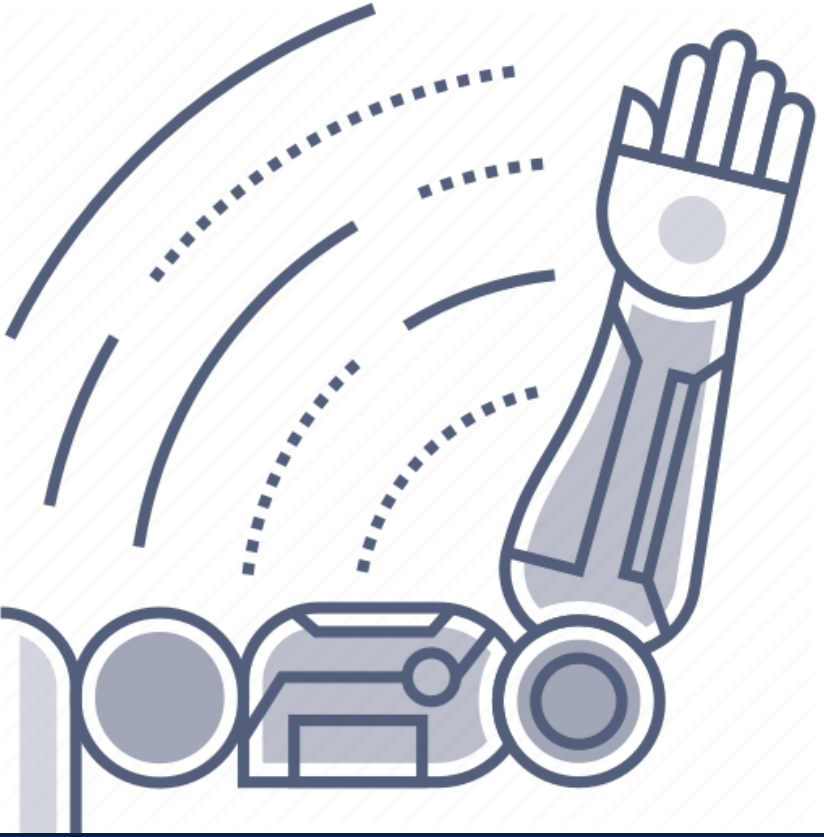
Менеджер поддержки продаж

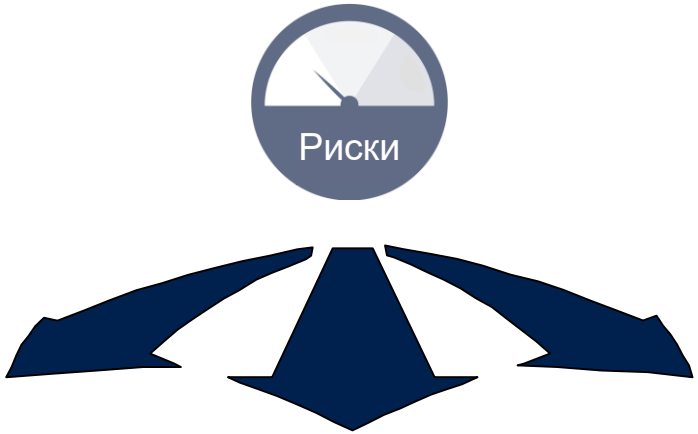
timur.guseynov@acronis-infoprotect.ru

Технологии



Технологии автоматизации процессов DLP





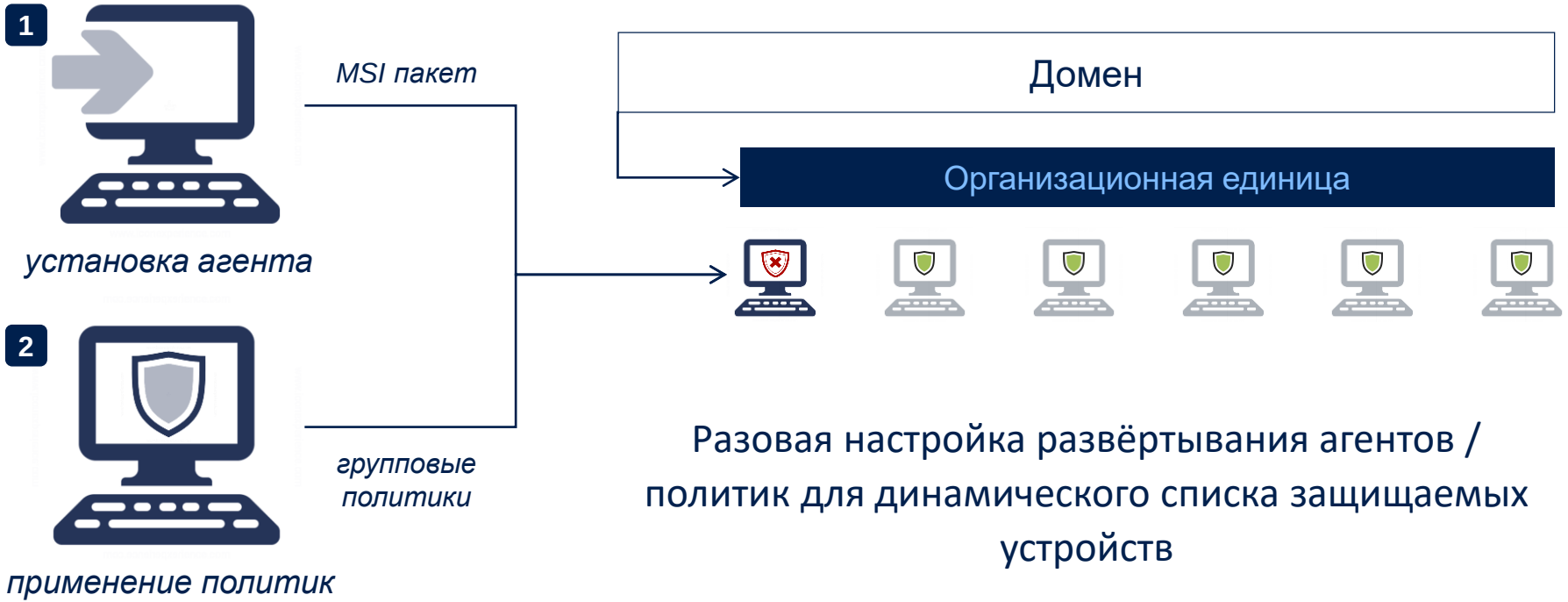
Исключение человеческих ошибок

Сокращение временных и трудозатрат на внедрение

Раннее выявление рисков

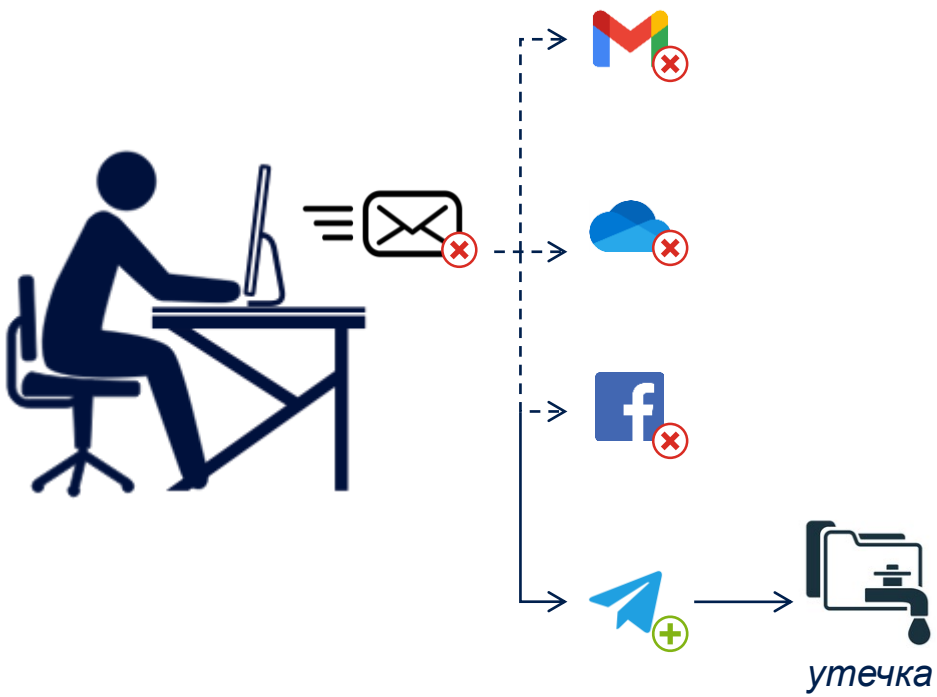
Автоматизация развёртывания политик безопасности

На примере DeviceLock DLP



Разовая настройка развёртывания агентов / политик для динамического списка защищаемых устройств

Распространённый алгоритм утечки



Типовые причины

1. Недостаток информированности пользователей об актуальной политике предотвращения утечек данных на предприятии

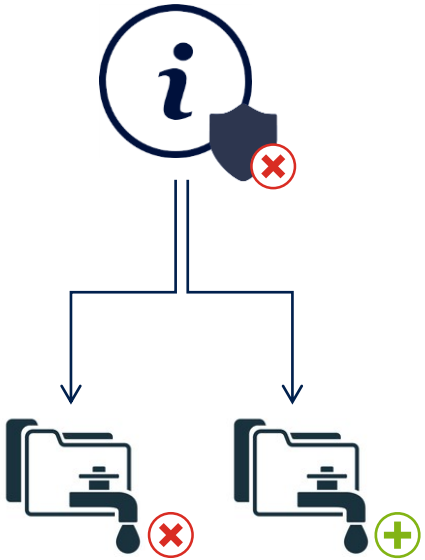
2. Реализация используемого решения DLP с фокусом на мониторинг утечек в отсутствие возможностей блокировки канала передачи и передаваемых по нему данных

Информирование сотрудников о политике DLP

Мера профилактики, возможная при условии сильной защиты решения DLP

Сильная самозащита

Слабая / отсутствующая самозащита

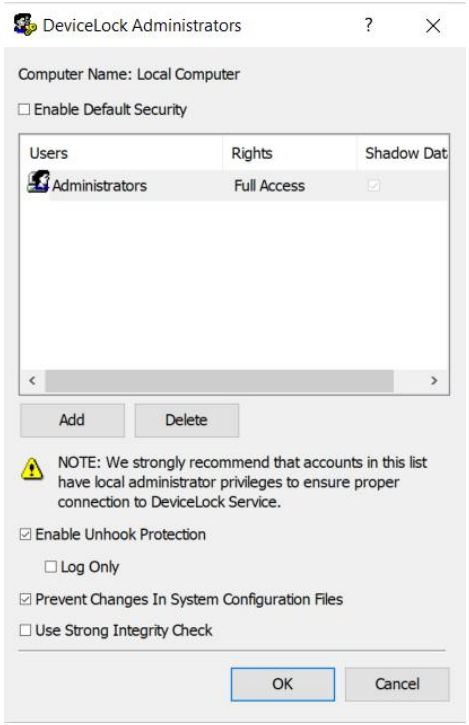


Технологии самозащиты

Защита решения DLP и связанных системных компонентов от отключения

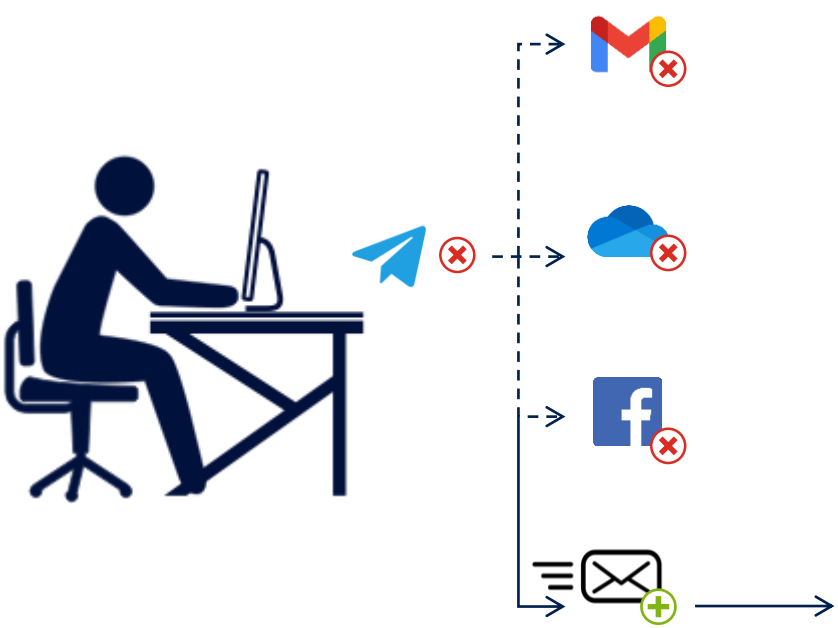
Защита системных компонентов от изменения

Проверка целостности компонентов решения DLPи связанных компонентов



Возможности блокировки

Перенаправляют активность пользователей в наилучшим образом контролируемые разрешённые каналы

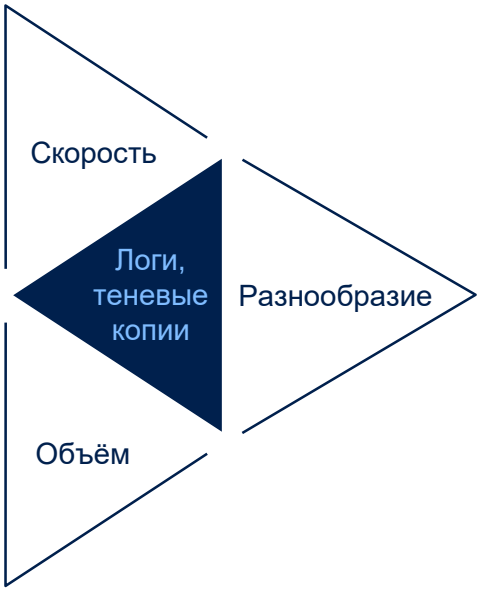


контентный анализ и фильтрация, теневое копирование, видеозапись действий пользователя

Раннее выявление рисков

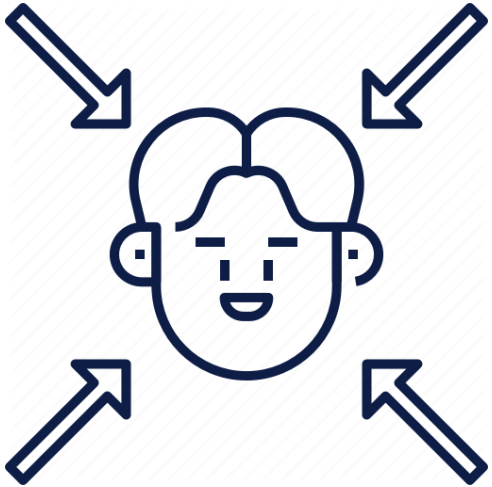
На базе анализа собираемых решением DLP данных

Большие данные уровня предприятия



Применение

Human-centric DLP



Аналитика на базе данных журналов

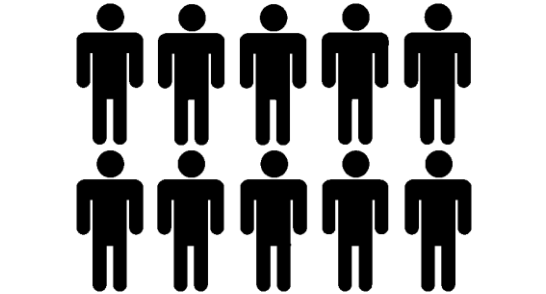
Пользователей, групп, сравнительная

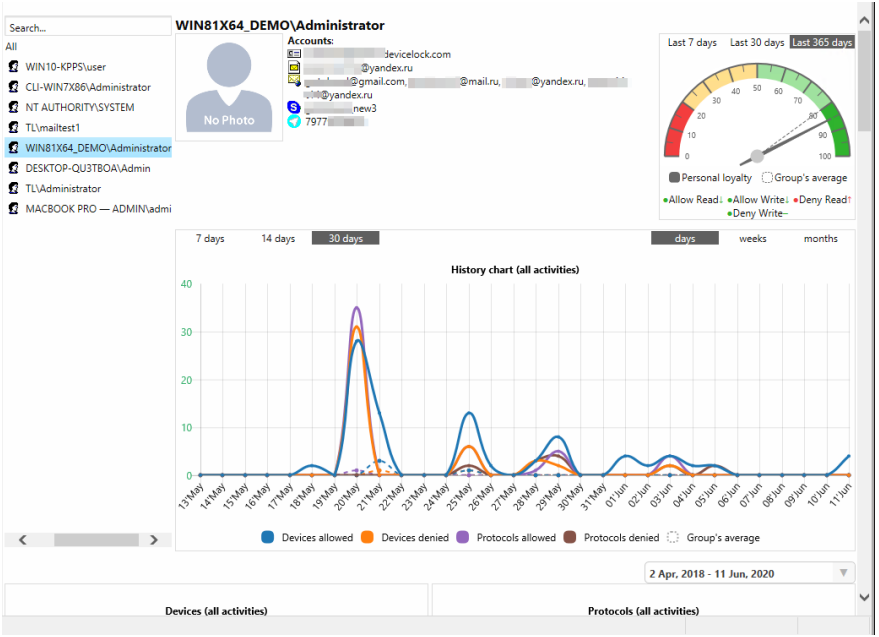
Профиль нормы

С нуля: 3-4 недели

Исторические данные

Выявление отклонений





Работа с контекстом

На примере возможностей модуля User Activity Monitor

Зачем

Реализация в DeviceLock DLP 9.0

Гибкая настройка правил записи по комбинации двух типов триггеров

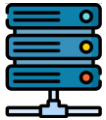
Системные

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

Резюмируя

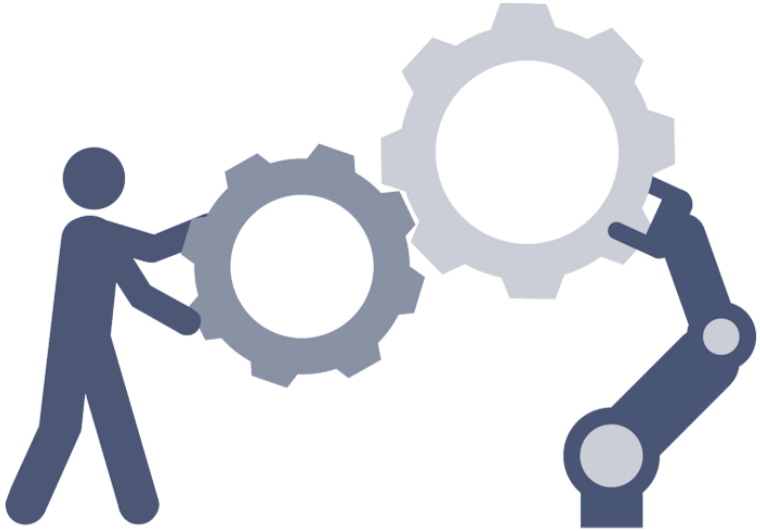
Люди

Разработка и внедрение политик DLP

Управление инцидентами, в т.ч. расследование и сбор доказательной базы

Управление рисками, в т.ч. выявленными соответствующими технологиями

Acronis DeviceLock



Обеспечение служб ИБ инструментами для работы в обоих направлениях

Технологии

Автоматизации развёртывания политик безопасности

Самозащиты DLP решения

Активного предотвращения утечек данных

Анализа генерируемого DLP слоя больших данных уровня предприятия

DeviceLock
AN ACRONIS COMPANY

Благодарю за внимание

Вопросы?

Тимур Гусейнов

Менеджер поддержки продаж

timur.guseynov@acronis-infoprotect.ru