

DLP для новой реальности

как спокойно спать в эпоху импортозамещения

Нормативная база импортозамещения

- В 2014 году в России объявлен курс на импортозамещение
- Приказ Министерства связи «Об утверждении плана по импортозамещению программного обеспечения» от 01.04.2015 № 96
- Постановление Правительства Российской Федерации от 16 ноября 2015 года № 1236 «Об установлении запрета на допуск иностранного программного обеспечения при закупках для государственных и муниципальных нужд»
- Директива о переходе на российское ПО до 2021 года, принятая в конце 2018 года
- Указ Президента РФ от 30 марта 2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации »



Единый реестр российских программ для электронных вычислительных машин и баз данных

К программному обеспечению, допускаемому к включению в реестр, относят программные продукты, удовлетворяющие следующим условиям:

- Российское юрлицо с российским контролем (более 50%)
- Технологическая независимость ПО (суверенитет разработки)
 - Наличие полных исходных кодов в России
 - Локальная инфраструктура разработки и сборки
 - Локальные специалисты, R&D и техническая поддержка
- Защита информации (суверенитет безопасности)
 - Контроль «закладок», утечек данных, устойчивости к взломам и т. п.
 - Доработки и сертификация продуктов по требованиям ФСТЭК, ФСБ и др.



Минцифры
России

ГОТОВЫ К ВЫЗОВАМ В НОВОЙ РЕАЛЬНОСТИ

- Уход иностранных IT-компаний
 - Остановка продаж ПО и продления лицензий на уже купленное ПО
 - Прекращение поддержки ПО
 - Увеличение угроз ИБ: количество атак растет, эмоциональный фон сотрудников оставляет желать лучшего
- Переход российских компаний на отечественные ОС и ПО



Инфраструктура Solar Dozor

Клиентская часть



- Astra Linux Special Edition версии 1.6 («Смоленск») и 1.7 («Орел», «Смоленск», «Воронеж»)
- Astra Linux Common Edition 2.12 («Орел»)
- Альт 8 СП
- Альт Рабочая станция 9
- РЕД ОС 7.2/7.3 («Муром»)
- Гослинукс ИК6
- CentOS 7/8
- Debian 10/11
- Ubuntu 18.04/20.04 LTS
- Linux Mint 20.3

Серверная часть

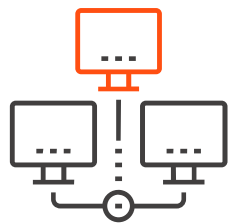


- Astra Linux Special Edition 1.6 («Смоленск»)
- CentOS 6.10, 7.9
- RHEL 6.10, 7.9

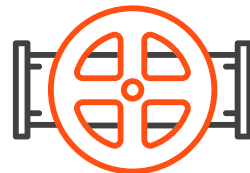


Поддержка СУБД PostgreSQL

Основные функциональные возможности Solar Dozor



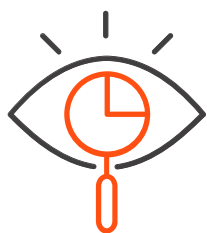
Контроль каналов передачи информации и коммуникаций



Предотвращение утечек информации



Широкие возможности поиска информации



Визуализация динамики нарушений



Контроль рабочего времени сотрудников



Ведение досье и формирование отчетов

Основные возможности Dozor Endpoint Agent

Функция (канал перехвата)	Windows	Linux	macOS*
Разрешение и блокировка подключения USB-устройств по заданным категориям и экземплярам	✓	✓	✓
Перехват сетевого трафика по протоколу HTTP(S), включая веб-почту и облачные хранилища	✓	✓	✓
Контроль почтовой переписки по протоколам SMTP, POP3, IMAP, в том числе с шифрованием SSL/TLS	✓	✓	✓
Контроль и блокировка печати	✓	✓	✓
Трансляция видео и снятие снимков с экрана	✓	✓	в разработке
Перехват нажатия клавиш (кейлогер)	✓	✓	в разработке
Контроль передачи данных через буфер обмена (текст, изображение, файлы)	✓	✓	в разработке
Контроль копирования файлов на USB-устройства и сетевые диски	✓	✓	в разработке
Контроль рабочего времени пользователей: название сайтов и приложений, время работы с ними, аналитика по сотруднику и отделу	✓	✓	в разработке
Запись звука с микрофона рабочей станции	✓	в разработке	в разработке
Перехват сообщений и файлов в мессенджерах	WhatsApp Telegram Viber Skype Zoom Webex Teams	WhatsApp Telegram	WhatsApp Skype

* Агент для Apple macOS выпущен в сентябре 2021 году и активно развивается

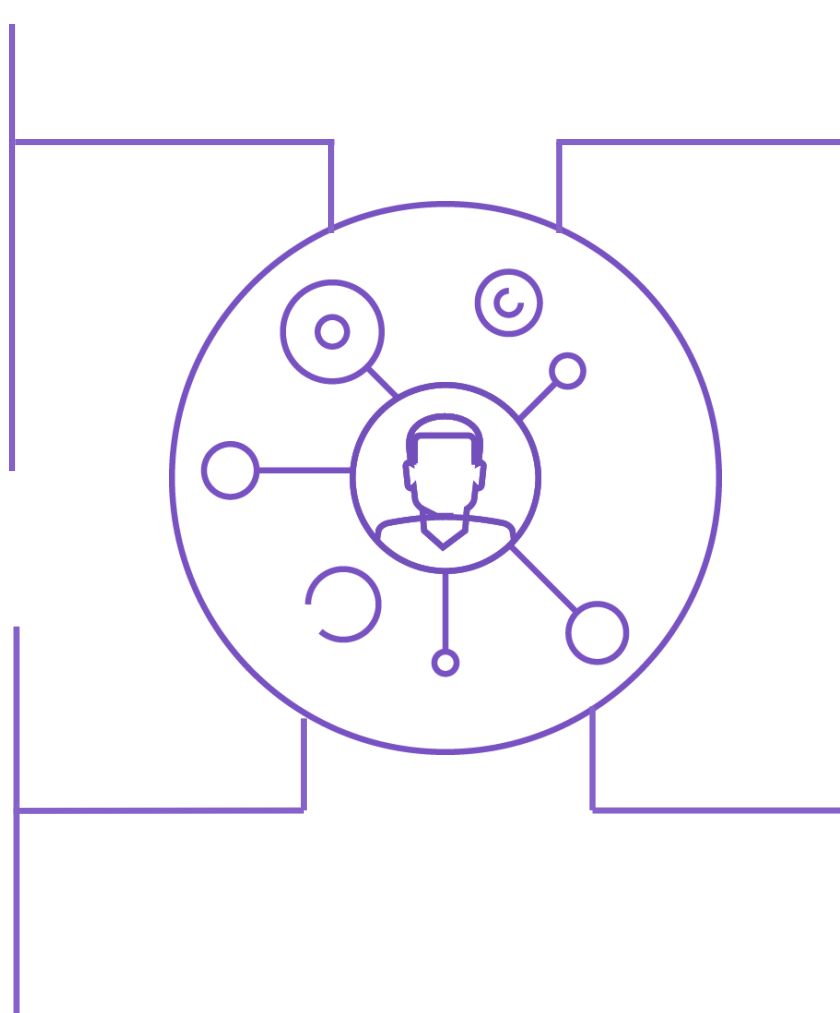
Расширенная аналитика (Dozor Dossier)

Интерактивные срезы информации

- Преднастроенная аналитика
- Визуальная статистика
- Возможность детального анализа каждого значения

Граф связей

- Карта внешних и внутренних контактов сотрудника
- Выявление устойчивых связей, нехарактерных контактов персоны



Сводный отчет по персоне

- Исчерпывающая информация о сотруднике в едином представлении
- Выявление аномалий коммуникаций, контактов, действий, нарушений персоны за указанный период времени

Контроль рабочего времени

- Активность сотрудника за рабочей станцией в рабочее и нерабочее время

Анализ поведения пользователей (User Behavior Analytics)

- На каждого сотрудника строится профиль характерных для него коммуникаций по приблизительно 20 параметрам — **профиль нормального поведения**
- Сами по себе наблюдаемые статистические показатели характера коммуникаций **обогащают досье сотрудника**
- Профиль нормального поведения позволяет детектировать **аномалии поведения**, которые являются триггерами для сотрудника службы безопасности
- Существуют определенные наборы характеристик поведения, под которые попадают определенные группы сотрудников — **паттерны поведения**.
Сейчас в системе 20 таких паттернов



Dozor vs Infowatch. Выполнение требований регуляторов



Есть компоненты иностранного ПО (модули Device Monitor и Person Monitor работают на ОС Windows Server)



Реализовано на ПО с открытым исходным кодом (включая ОС и СУБД), что полностью соответствует Постановлению Правительства от 16 сентября 2016 года №925

Выгоды: отсутствие иностранных компонентов и регистрация в Едином реестре отечественного ПО позволят полностью соответствовать законодательству и требованиям регуляторов, что позволяет использовать Solar Dozor для соответствия стандартам защиты персональных данных и коммерческой тайны, а также в полной мере реализовывать программу импортозамещения.

Dozor vs SearhInform. Выполнение требований регуляторов

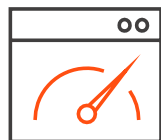


Установка серверной части и базы данных поддерживается только на компонентах Windows (MS Windows Server и MS SQL Server соответственно)

Реализовано на ПО с открытым исходным кодом (включая ОС и СУБД), что полностью соответствует Постановлению Правительства от 16 сентября 2016 года №925

Выгоды: отсутствие иностранных компонентов и регистрация в Едином реестре отечественного ПО позволят полностью соответствовать законодательству и требованиям регуляторов, что позволяет использовать Solar Dozor для соответствия стандартам защиты персональных данных и коммерческой тайны, а также в полной мере реализовывать программу импортозамещения

Подтвержденная надежность Solar Dozor



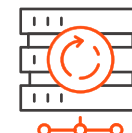
Производительность

- Поиск среди 17 млн сообщений за 1 сек
- Подтвержденная укладка в архив — 2,7 ТБ в сутки
- Корпоративная почта — 200 Гбит/час
- Сетевой трафик — 600 Мбит/сек
- Контроль сетевых хранилищ — 1,8 Тбит/сутки
- Долговременный архив — 1000+ ТБ
- Подтвержденные сроки хранения архива коммуникаций — 10+ лет



Масштабируемость

- Полнофункциональная поддержка территориально распределенной инфраструктуры
- Объединение нескольких инсталляций в единый кластер с централизованным управлением
- Конфигурирование системы и настройка правил фильтрации могут выполняться специалистами центрального офиса
- Гибкое управление нагрузкой на каналы передачи данных обеспечивает комфортное функционирование даже при слабой пропускной способности каналов



Отказоустойчивость

- Подтвержденная инсталляция на 250 000+ агентов
- Работа в кластерном режиме, регулярная самодиагностика. Данные диагностики распределенных узлов можно отследить в реальном времени
- Доступно ежедневное резервное копирование всех компонентов системы и хранение резервных копий на выделенном сервере

Дополнительные преимущества

- Индивидуальный подход к заказчикам, помощь и консультирование на всех этапах взаимодействия
- Большие возможности интеграции системы внутри продуктовой линейки Solar и за ее пределами
- Доработка функциональных возможностей продукта в рамках взаимодействия с заказчиками





Центральный офис

**125009, Москва, Никитский
переулок, 7с1**

+7 (499) 755-07-70

solar@rt-solar.ru

