Solar Dozor

Предотвращение утечек информации,
профилактика инцидентов ИБ и проведение расследований

rt-solar.ru
rt.ru

Ростелеком
Солар

Solar Dozor

Solar Dozor — система для предотвращения утечек конфиденциальной информации (Data Leak Prevention, DLP). Она обеспечивает контроль коммуникаций сотрудников, возможность блокировки или модификации нежелательных сообщений, выявление и мониторинг групп риска, а также ретроспективный анализ архива коммуникаций для проведения расследований.

Кроме того, Solar Dozor анализирует поведение пользователей (User Behavior Analytics) и выявляет в нем аномалии, определяет круг общения и приватные контакты сотрудников, а также профилирует их на основе 20 устойчивых паттернов поведения.

Если организация состоит из нескольких дочерних зависимых обществ или территориально распределенных филиалов, инсталляции Solar Dozor могут работать как единое целое (функции модуля MultiDozor).

120+ сотрудников — крупнейшая команда в России

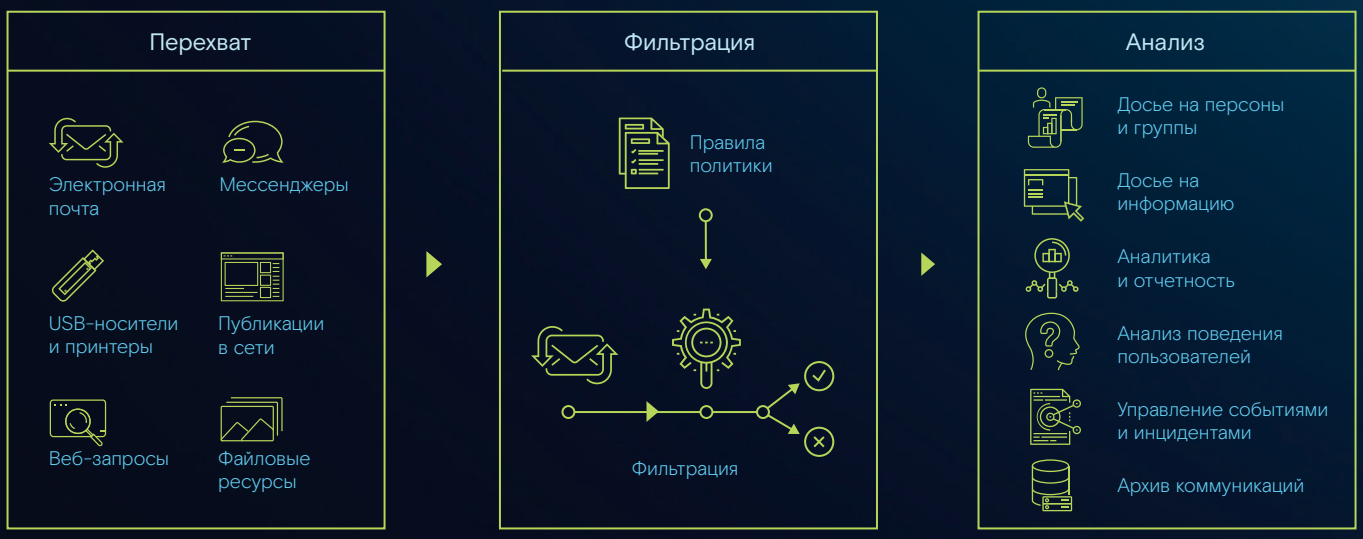
300+ тысяч — подтвержденное число агентов в одной инсталляции

600+ проектов — в крупнейших государственных и коммерческих организациях

1000 тб — подтвержденный объем архива у клиента

- Отработанная методология внедрения и эксплуатации DLP-системы
- Развитые визуальные инструменты и графические отчеты
- Единый веб-интерфейс и единая политика безопасности
- Полнофункциональные агенты для Windows, Linux, macOS

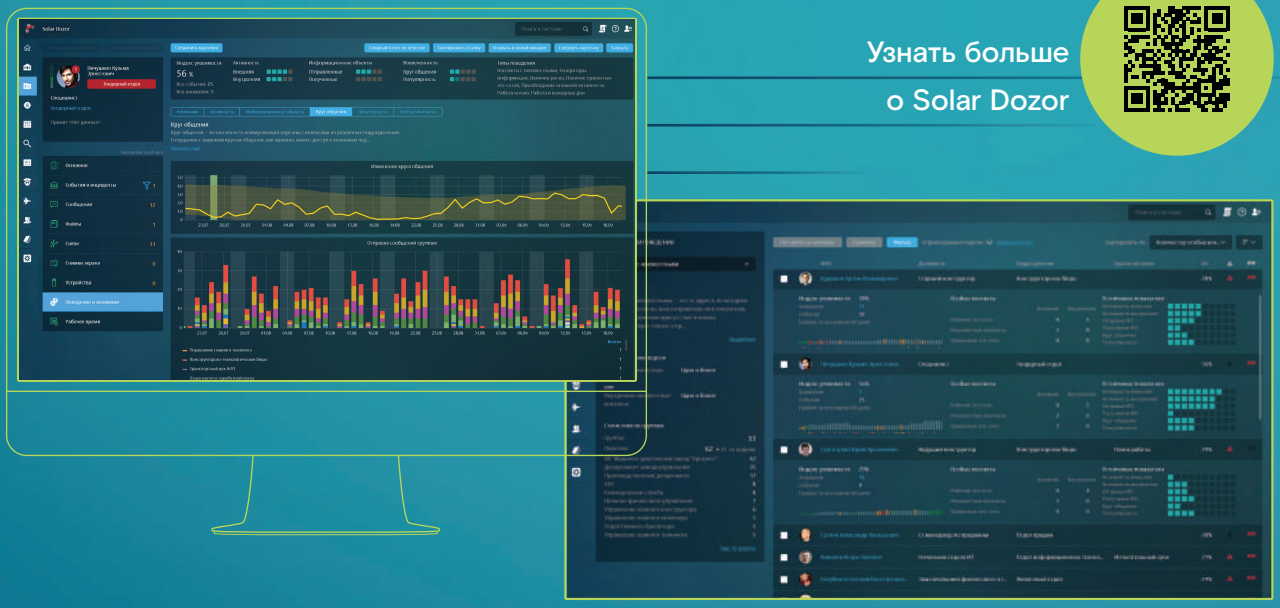
Принцип работы



Решаемые задачи

- Профилактика инцидентов ИБ
- Проведение расследований
- Выявление признаков корпоративного мошенничества
- Мониторинг коммуникаций сотрудников
- Отслеживание аномалий поведения
- Выявление и мониторинг групп риска
- Профилактика экстремизма и терроризма
- Управление конфликтом интересов

Взаимодействие с Solar Dozor



Узнать больше
о Solar Dozor

Возможности

Контроль каналов коммуникации и предотвращение утечек информации

- Электронная почта
- Социальные сети и мессенджеры
- USB-носители и принтеры
- Веб-сервисы
- Облачные и локальные файловые хранилища

Выявление ранних признаков корпоративного мошенничества и проведение расследований

- Мгновенный поиск по архиву
- Перефильтрация архива
- Досье на персону
- Мониторинг групп особого контроля

Ведение досье по персонам, анализ связанной с ними информации

- Граф связей
- Анализ поведения пользователей
- Скриншоты рабочего стола
- Контроль рабочего времени
- Используемые USB-устройства
- Запись звука с рабочей станции

Выявление аномальной активности и профилирование сотрудников

- Рабочие и приватные контакты
- Паттерны поведения
- Поиск похожих персон
- Мониторинг групп риска
- Индекс уязвимости сотрудника

Эффективное управление событиями и инцидентами

- Инцидентная модель в соответствии с ГОСТ 15408 «Менеджмент ИБ»
- Развитая ролевая модель
- История работы с инцидентом
- Уровни критичности инцидентов

Построение отчетов по событиям и инцидентам

- Тепловая карта коммуникаций
- Сводный отчет по персоне
- Отчет по отправителям и получателям информации
- Сводный отчет по инцидентам

Поддержка территориально распределенной структуры организации

- Централизованный контроль деятельности сотрудников в сети филиалов (организаций)
- Работа с данными разрозненных филиалов (организаций) как с единым целым
- Централизованные настройка и распространение политики безопасности по сети филиалов (организаций)

Преимущества Solar Dozor

Эффективный перехват и блокировка

- Возможность перехвата основного трафика на сетевом шлюзе снижает нагрузку на рабочие станции сотрудников
- Возможность установки «в разрыв» для блокирования утечек при больших потоках трафика
- Изменение или удаление содержимого сообщений электронной почты предотвращает утечки

Снижение ложных срабатываний

- Мониторинг действий сотрудников для превентивного обнаружения угроз
- Внимание аналитика фокусируется на потенциальных угрозах и сотрудниках из групп риска
- События и инциденты легко фильтруются и сортируются для максимального сужения выборки
- Данные размечаются тегами по аналогии с поисковиками и социальными сетями

Гибкость, стабильность и производительность

- Встраивается в любую инфраструктуру без конфликтов с другим ПО
- Позволяет реализовать любую программу хранения данных в соответствии с имеющимися мощностями
- Поддерживает модель здоровья Zabbix

Подходит для импортозамещения

- Все модули могут работать на свободных дистрибутивах ОС GNU/Linux
- Полнофункциональный агент для ПК с ОС Linux
- Участник Единого реестра отечественного ПО (№ 1480)
- Сертификат соответствия ФСТЭК России № 4459

Контроль распределенных филиалов (MultiDozor)

- Все функции Solar Dozor доступны в территориально распределенном режиме
- Единое досье с данными о сотрудниках всей организации
- Сквозной мониторинг групп сотрудников по организации
- Разграничение прав доступа офицеров безопасности
- Архитектурная гибкость и сниженная нагрузка на каналы передачи данных

Ключевые клиенты

Ростелеком Солар

solar@rt-solar.ru rt.ru rt-solar.ru

+7 (499) 755-07-70