ОПИСАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Функциональные характеристики

Продукт: СОПКА.Рой · Версия: 1.0.0 · Агент: 1.0.1 · Протокол: 1 · Редакция: 15.10.2026

Правообладатель ПО: Общество с ограниченной ответственностью «Каннам». ИНН 2543020645, ОГРН 1132543001502. Реквизиты приведены в отдельном разделе документации.

Назначение

СОПКА.Рой - программный комплекс класса DLP для SaaS, локального или выделенного развёртывания по договору и централизованного контроля событий на рабочих станциях Windows. Агенты оценивают полученные политики и выполняют доступные действия; сервер принимает телеметрию, хранит результаты, формирует инциденты и предоставляет веб-интерфейс для анализа и расследования. Клиентская версия 1.0.0 предназначена для Windows.

Область применения

- контроль корпоративных рабочих станций, находящихся под управлением организации;
- выявление передачи чувствительных данных через контролируемые каналы;
- учёт событий приложений, файлов, буфера обмена, USB-устройств и сетевых интерфейсов;
- поиск уже существующих файлов по заданиям администратора;
- расследование инцидентов с фиксацией статуса, ответственного и комментариев;
- централизованное управление политиками и версиями Windows-агентов.

Функции версии 1.0.0

Подсистема	Возможности
Рабочие области	Изоляция клиентов, политик, событий, инцидентов, пользователей и настроек по workspace.
Агенты	Регистрация по ключу, уникальный UUID, heartbeat, получение политик, служебных команд и контроль версии протокола.

Подсистема	Возможности
События	Приём и нормализация файловых, USB-, clipboard-, application-, network-, browser- и иных событий.
Политики	Семь редакторов каналов с условиями, приоритетами политики и правила: наблюдение (audit), применение явных действий (deny) и исключение выбранных действий (allow). Подробные поля и ограничения приведены в «Политиках и каналах контроля».
Инциденты	Отдельная сущность, создаваемая по решению политики; статусы, комментарии, ответственный и история изменений.
Поиск файлов	Задания, расписания, области сканирования, метки, watchlist, карточка файла, версии, предпросмотр и контролируемая загрузка.
Экран	Ручной запрос снимка, периодические снимки по разрешению функции и заданному интервалу в возможностях, прямой экран по явной команде уполномоченного пользователя.
Уровни доступа	Роли admin, editor и viewer; приглашения в рабочую область; разграничение полномочий и изоляция данных организаций.

Правовые и организационные условия эксплуатации

СОПКА.Рой предоставляет технические функции контроля и не определяет правовое основание их применения. Эксплуатирующая организация самостоятельно определяет цели и основания обработки, перечень контролируемых каналов, категории данных, сроки хранения, локальные акты и круг уполномоченных пользователей.

- обработка должна быть законной, целевой и не избыточной по отношению к заявленным задачам;
- работники знакомятся с применимыми локальными актами и правилами использования корпоративных информационных ресурсов;
- снимки экрана, прямой экран, клавиатурные события и загрузка файлов включаются только при документированной необходимости и ограниченном ролевом доступе;

- заказчик продукта отвечает за соблюдение требований законодательства и внутренних процедур при эксплуатации системы.

Установка и сопровождение агента

Агент устанавливается по регистрационному ключу, который создаётся в рабочей области. Пакет агента не привязан к рабочей области: регистрационный ключ передаётся отдельно при установке. После установки клиент регистрируется на сервере, получает device-токен, отправляет heartbeat и забирает подписанный bundle политик.

Поставка и развёртывание выполняются в рамках договора: состав включённых модулей, каналы контроля, сроки хранения и доступ администраторов фиксируются организационными документами заказчика.

Основной Windows-пакет установки и сопровождения - CopkaRoySetup.exe. При обновлении EXE проверяется контрольная сумма; отдельный ZIP-updater с подписанным манифестом относится к legacy-сценарию. Наличие механизма обновления не означает публикацию другой версии продукта: текущий документ описывает только 1.0.0.

Ограничения

- агент версии 1.0.0 рассчитан на Windows x64 и устанавливается с правами администратора;
- Linux-агент в состав версии 1.0.0 не входит;
- фактическое блокирование зависит от возможностей конкретного клиентского модуля; часть правил работает в режиме аудита или оповещения;
- клавиатурный контроль зависит от возможностей и настроек агента, а прямой экран запускается вручную;
- внешнее TLS-терминирование, резервное копирование и защита публичного контура настраиваются администратором;
- продукт не заявляется как сертифицированное средство защиты информации или средство криптографической защиты.

Границы контроля

Событие, инцидент и выполненное действие - разные результаты. Событие фиксирует наблюдение; инцидент создаётся при соответствующем решении политики; команда требует подтверждённого результата агента. Отсутствие инцидента само по себе не доказывает отсутствие события или утечки.

Фактический набор функций определяется лицензированным составом поставки, настройками workspace, ролью и capabilities клиента. Прямой экран предоставляет просмотр без удалённого ввода мыши и клавиатуры. Для приёмки проверьте нужные каналы на тестовой группе с согласованными примерами.

Интеграции

API рабочей области находится в разработке, по умолчанию отключён и не является стабильным интерфейсом для рабочих интеграций. API агента и внутренние запросы веб-консоли имеют отдельное назначение.

Как читать функциональный состав

Состав функций разделяется на наблюдение, выявление по политикам, расследование и реагирование. Для каждой функции в документе «Возможности каналов» указаны назначение и ограничения; поддерживаемые автоматические действия перечислены в «Политиках и каналах контроля». Контроль интерфейсов сети не равен анализу всех пакетов, наблюдение браузера не гарантирует извлечение любого веб-содержимого, инвентаризация ПО не выполняет его автоматическое удаление.

Поставка и проверка результата

Общие сценарии доступны в SaaS и локальном контуре с учётом роли и состава поставки. Наличие функции в каталоге не подтверждает её готовность на конкретном компьютере: проверяют версию агента, разрешение, пользовательскую сессию и фактический результат. Для приёмки используют согласованные тестовые примеры по каждому требуемому каналу.

Масштаб и ресурсный профиль

Расчёт на 1000 одновременно работающих агентов приведён в «Системных требованиях» с частотами обмена, событий и снимков. Это начальный ресурсный бюджет для испытания, а не гарантированное число клиентов или подтверждённый SLA. Состав каналов и срок хранения входят в расчёт нагрузки.

AI-анализ данных безопасности

AI-чат связывает данные компьютеров, событий, инцидентов, групп, политик, возможностей, команд и поиска файлов. Инструменты читают данные с проверкой прав, создают PDF по явной просьбе и готовят подтверждение команды. Отправку команды разрешает пользователь кнопкой под ответом; результат проверяется по истории команд.

Подробнее: AI-чат: анализ безопасности.