

R-Vision Endpoint

Сбор данных, обнаружение и реагирование
на конечных устройствах



R-Vision

R-Vision Endpoint — ключевой компонент экосистемы R-Vision EVO, который расширяет функциональные возможности других технологий и предоставляет дополнительные преимущества от их использования.

Благодаря R-Vision Endpoint можно проводить детализированную инвентаризацию активов, выявлять киберугрозы и осуществлять реагирование на инциденты непосредственно на конечных устройствах, а также автоматически проводить технический аудит всех популярных типов ОС на соответствие стандартам информационной безопасности.

Схема работы R-Vision Endpoint



Задачи, которые решает R-Vision Endpoint совместно с технологиями R-Vision



R-Vision SGRC

Оперативная инвентаризация активов, технический аудит соответствия стандартам ИБ



R-Vision LM

Сбор событий с конечных устройств для нормализации и хранения



R-Vision UEBA

Передача событий с конечных устройств для выявления аномалий



R-Vision VM

Предоставление сведений об уязвимостях с конечных устройств



R-Vision TIP

Получение индикаторов компрометации с конечных устройств и обогащение дополнительным контекстом



R-Vision SOAR

Реагирование и выполнение действий на конечных устройствах, оперативная инвентаризация активов



R-Vision TDP

Управление ложной инфраструктурой, сбор данных для анализа действий злоумышленника и цифровая гигиена хостов



Расширенная инвентаризация с R-Vision SOAR и R-Vision SGRC

R Vision Endpoint расширяет инвентаризационные возможности технологий R-Vision SOAR и R-Vision SGRC, позволяя:

- получать информацию об изменениях ПО и ОС без привилегированного доступа
- автоматически передавать информацию об изменениях с конечных устройств на сервер в режиме реального времени
- расширить спектр инвентаризируемых активов, осуществляя поиск и инвентаризацию устройств, находящихся в том числе за пределами NAT/VPN



Сбор событий для R-Vision LM и R-Vision UEBA

Все события информационной безопасности, прикладного программного обеспечения, события системы и связанная с ними телеметрия передаются с конечных устройств в R-Vision LM для нормализации, анализа и хранения. События, в ходе которых использовались определенные техники и тактики из матрицы MITRE ATT&CK, помечаются специальными тегами для ускорения процесса расследования.

Связанные с поведением системы и пользователя в ней события, передаются в R-Vision UEBA для выявления нарушений в состоянии ИТ и ИБ-систем. Компонент R Vision Endpoint упрощает процесс получения событий с хостов путем централизованного управления политикой сбора, в том числе на Linux-системах.



Предоставление сведений об уязвимостях в R-Vision VM

Информация об уязвимом программном обеспечении, собранная с конечных устройств, передается в R-Vision VM для осуществления приоритизации уязвимостей и контроля их устранения.



Передача индикаторов компрометации в R-Vision TIP

Хэш-суммы вредоносных файлов, находящиеся на конечных устройствах, сравниваются с базой индикаторов компрометации из R-Vision TIP, обогащаются дополнительным контекстом, связанным с этой вредоносной сущностью, и передаются в R-Vision SOAR для осуществления реагирования.



Оперативное реагирование на инциденты на хостах с R-Vision SOAR

R-Vision Endpoint упрощает процесс реагирования на инциденты при использовании совместно с R-Vision SOAR, позволяя выполнять действия на конечных устройствах вручную и автоматически:

- сетевая изоляция хоста
- отправка файлов во внешние системы для проверки
- остановка процесса
- удаление файлов



Технический аудит ИБ с R-Vision SGRC

Информация о настройке параметров безопасности в операционных системах и прикладном программном обеспечении собирается с конечных устройств в автоматическом режиме для проведения аудита соответствия стандартам информационной безопасности. R-Vision Endpoint поддерживает проверки для большинства популярных типов ОС (Windows, Linux, Mac OS) и ПО.



Управление ложной инфраструктурой в R-Vision TDP

R-Vision Endpoint позволяет размещать приманки, созданные в R-Vision TDP, агентским способом независимо от типа операционных систем конечного устройства. Агенты, установленные на защищаемых устройствах, дают возможность упростить процесс администрирования ложной инфраструктуры, получать данные для анализа действий злоумышленника, а также осуществлять процесс цифровой гигиены на конечных устройствах.



О компании

R-Vision – разработчик систем кибербезопасности. Компания с 2011 года создает технологии, которые помогают бизнесу и государственным организациям по всему миру уверенно противостоять актуальным киберугрозам и обеспечивать надежное управление информационной безопасностью.

Технологии **R-Vision** используются в банках, государственных организациях, нефтегазовой отрасли, энергетике, металлургии, промышленности и компаниях других отраслей.

 rvision.ru

 sales@rvision.ru

 +7 (499) 322 80 40

Дайджест информационной безопасности:
rvision.ru/blog

 t.me/rvision_pro

 [/rvision_ru](https://vk.com/rvision_ru)

 [/RVisionPro](https://www.youtube.com/RVisionPro)