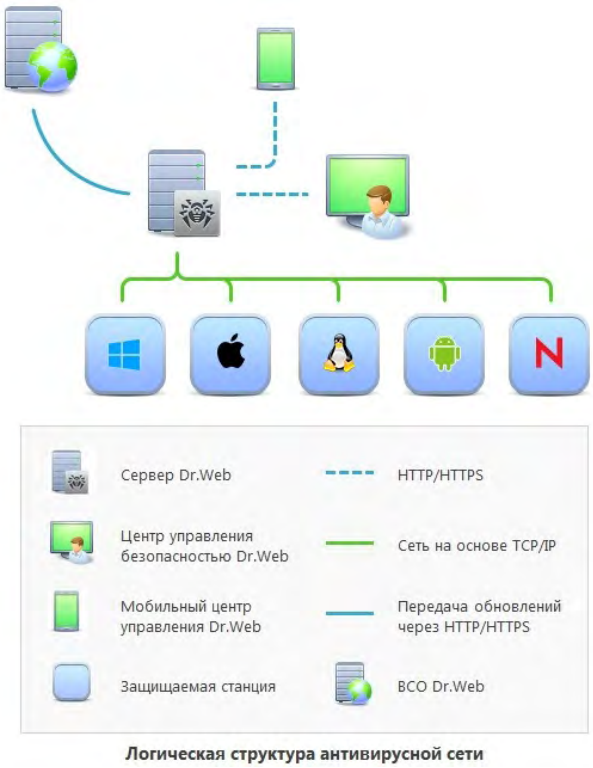
Dr.WEB®
с 1992 года

О возможности интеграции Dr.Web Enterprise Security Suite 11 с программным обеспечением для управления событиями информационной безопасности (SIEM)

О возможности интеграции Dr.Web Enterprise Security Suite 11 с программным обеспечением для управления событиями информационной безопасности (SIEM)

Dr.Web Enterprise Security Suite (далее — ESS) обладает широкими возможностями централизованного управления антивирусной защитой организации, обеспечивая своевременное обнаружение и предотвращение вирусозависимых компьютерных инцидентов.



Логическая структура антивирусной сети

ESS осуществляет подробное протоколирование работы компонентов антивирусного ПО, а также событий, влияющих на информационную безопасность в режиме реального времени, что позволяет использовать серверы Dr.Web ESS в качестве одного из источников критических данных для систем управления событиями информационной безопасности (Security information and event management, SIEM).

Интеграция сервера Dr.Web ESS с SIEM-системами осуществляется посредством Web API, который использует протокол HTTP(S). Web API принимает HTTP-запросы и возвращает ответ в формате XML (по умолчанию) или JSON.

Широкие функциональные возможности Web API позволяют передавать в SIEM-системы информацию о работе различных компонентов антивирусной сети организации, в том числе:

- список компонентов и модулей защиты, установленных/запущенных на антивирусных агентах;
- текущий список антивирусных баз, установленных на агентах для контроля их актуальности;

- текущий статус антивирусного агента либо агентов в пользовательской группе (в сети / не в сети / новый / удаленный / имеет ошибки обновления и т. п.);
- список (топ) обнаруженных угроз (вредоносного ПО) за период на выделенном агенте / в пользовательской группе или общий по всем защищаемым объектам;
- состояние карантина на защищаемом объекте (агенте) / суммарно по пользовательским группам за период. Включает в себя информацию о событии перемещения объектов в карантин, данные о сработавшем компоненте и о самом вредоносном объекте);
- информацию об антивирусных агентах-новичках (впервые авторизованных на ES-сервере);
- данные о местоположении антивирусных агентов, установленных на защищаемые объекты, включая мобильные устройства;
- список пользовательских групп, а также антивирусных агентов в составе пользовательских групп, и их статус (в сети / не в сети / удалена / новая / с ошибками обновления ПО и пр.);
- статистку сервера по результатам антивирусного сканирования защищаемого объекта;
- состояние репозитория ES-сервера, включая информацию о продуктах в репозитории, даты последнего обновления, номера ревизии и его кода;
- список администраторов, имеющих доступ к антивирусному серверу;
- статистику сервера по использованным ресурсам, включая количество антивирусных агентов всего / в онлайне, выделенной памяти и прочих параметров для мониторинга технического состояния сервера.

Если SIEM-система поддерживает возможность генерации оповещений (тревог) о текущих проблемах с безопасностью и трансляцию их на внешние приложения средствами API, то ES-сервер может обеспечить передачу их конечным пользователям и отображение сообщений в виде всплывающих окон (ПК) / push-уведомлений (в Android).

После отправки сообщений на антивирусный агент ES-сервер формирует статус доставки (инициирована / завершилась с ошибкой / отложена) и передает его средствами API в SIEM-систему.

Подробное описание форматов XML/JSON представлено в Руководстве администратора Dr.Web Enterprise Security Suite.

При возникновении вопросов по интеграции ESS с внешними приложениями обращайтесь в службу поддержки.

О компании «Доктор Веб»

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года. Все права на технологии Dr.Web принадлежат компании «Доктор Веб». «Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ, имеет свою антивирусную лабораторию, глобальную службу вирусного мониторинга и службу технической поддержки, которые расположены в России.

Компания «Доктор Веб» — ключевой игрок на российском рынке программных средств обеспечения базовой потребности бизнеса — безопасности информации. Свой выбор в пользу продуктов Dr.Web сделали Государственная Дума Федерального Собрания РФ, ЦИК России, Минобороны России, Верховный Суд РФ, Совет Федерации Федерального Собрания РФ, Центральный банк Российской Федерации, многие другие государственные учреждения и крупнейшие компании.
Вот только некоторые клиенты Dr.Web: https://customers.drweb.com.

Dr.Web внесен в «Единый реестр российских программ для электронных вычислительных машин и баз данных» **Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации.**

Использование отечественного антивирусного ПО Dr.Web обеспечивает нашим клиентам защиту от рисков, связанных с изменением международной обстановки, таких как отказ в использовании, продлении, поставке или получении обновлений, а также от угроз, созданных для целенаправленных атак на предприятия и граждан России.

Со знаком качества

- «Доктор Веб» имеет сертификаты, позволяющие использовать ПО Dr.Web в организациях с повышенными требованиями к уровню безопасности.
- Dr.Web сертифицирован на отсутствие недекларированных возможностей – по 2 уровню контроля, на соответствие требованиям документа «Требования к средствам антивирусной защиты», утв. приказом ФСТЭК России № 28 от 20.03.2012 г., на соответствие требованиям ФСБ России к антивирусным средствам.
- Продукты Dr.Web применяются для защиты информации, содержащейся в различных информационных системах, в том числе информации ограниченного доступа (государственная тайна, персональные данные и т. д.).
- Использование ПО Dr.Web позволяет обеспечить надлежащее выполнение требований норм законодательства РФ о применении мер для защиты:
  – информации с ограниченным доступом (государственная тайна, персональные данные и т. д.);
  – отдельных категорий граждан от информации, причиняющей вред.

Сертификаты ФСТЭК России	**Сертификаты Минобороны России**	**Сертификаты ФСБ России**	**Все сертификаты и товарные знаки**

Государственные сертификаты и награды, а также география пользователей Dr.Web свидетельствуют о высоком качестве продуктов, созданных талантливыми российскими программистами.

125040, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12а
Тел.: +7 495 789–45–87 (многоканальный)
Факс: +7 495 789–45–97
https://антивирус.рф | https://www.drweb.ru | https://curenet.drweb.ru | https://free.drweb.ru