



Kaspersky EDR для бизнеса Оптимальный

Список функций

kaspersky

Содержание

- Защита рабочих мест
страница 3
- Управление безопасностью
страница 4
- Базовые функции EDR
страница 5
- Поддерживаемые устройства и операционные системы
страница 8
- Поддержка нескольких клиентов
страница 8



Защита рабочих мест

Функция	Описание
Многоуровневая защита от вредоносного ПО	Последние технологии «Лаборатории Касперского» сочетают сигнатурную защиту, эвристический и поведенческий анализ, машинное обучение и облачные возможности для защиты рабочих станций Windows, Linux и MacOS от известных, неизвестных и продвинуток угроз. Использование шаблонов сигнатур позволяет повысить уровень обнаружения вредоносных программ и одновременно уменьшить размер файлов обновлений и освободить каналы связи для других задач.
Поведенческий анализ	Собирает информацию о действиях приложений на компьютере пользователя и передает ее другим компонентам решения для более надежной защиты.
Защита от эксплойтов	Отслеживает исполняемые файлы, запускаемые уязвимыми приложениями. При попытке запустить исполняемый файл уязвимым приложением без участия пользователя этот компонент блокирует исполнение файла.
Адаптивный контроль аномалий	Отслеживает и блокирует операции, нетипичные для компьютеров корпоративной сети. Для выявления подозрительного поведения (например, запуск Microsoft PowerShell из офисного приложения) используется набор правил, разработанный экспертами «Лаборатории Касперского» с учетом типичных сценариев вредоносной активности.
Откат вредоносных действий	Обеспечивает лучшую защиту от шифровальщиков, устраняя последствия работы вредоносного ПО для операционной системы, в том числе действий с файлами, реестром, системой и сетевым окружением. При откате модуль работает со строго определенным набором данных и не приводит к сбоям в работе операционной системы или нарушению целостности данных.
Защита от файловых угроз	Антивирус эффективно обнаруживает и удаляет угрозы на устройствах в режиме реального времени с использованием как антивирусных баз самого приложения, так и глобальной облачной базы Kaspersky Security Network.
Защита от почтовых угроз	Этот компонент приложения проверяет входящие и исходящие электронные сообщения на наличие угроз. Он начинает работать при запуске приложения, находится в оперативной памяти устройства и проверяет все сообщения, отправляемые и получаемые по протоколам POP3, SMTP, IMAP и NNTP.
Защита от веб-угроз	Этот компонент защищает входящие и исходящие данные, передаваемые по протоколам HTTP, HTTPS и FTP, и блокирует выполнение опасных скриптов на устройстве.
Сетевой экран	Сетевой экран защищает все конечные устройства от сетевых угроз при просмотре веб-сайтов и работе в локальной сети. Он пресекает несанкционированные сетевые соединения, снижая риск заражения компьютера, отслеживает сетевую активность приложений, препятствуя распространению вредоносного ПО по сети, а также блокирует случайные и преднамеренные действия пользователей, нарушающие политику безопасности.
Система предотвращения вторжений (HIPS)	Блокирует действия приложений, которые могут повредить операционную систему, и контролирует доступ к ресурсам операционной системы и личным данным.
Защита от сетевых угроз	Этот компонент проверяет входящий сетевой трафик на наличие активности, типичной для сетевых атак, таких, например, как вмешательство удаленного устройства в работу операционной системы. При обнаружении попытки сетевой атаки защита от сетевых угроз блокирует сетевую активность, направленную с атакующего компьютера.
Защита от атак BadUSB	Не допускает подключения к компьютеру зараженных USB-устройств, имитирующих клавиатуру. Когда к компьютеру подключается USB-устройство, определяемое операционной системой как клавиатура, приложение генерирует цифровой код и предлагает пользователю ввести его. Эта процедура называется авторизацией клавиатуры.
Защита AMSI	Поддерживает интерфейс сканирования Microsoft на вредоносные программы (AMSI). Этот интерфейс позволяет сторонним программам, использующим AMSI, отправлять объекты (например, скрипты PowerShell) в Kaspersky Endpoint Security для дополнительной проверки и получать результаты проверки этих объектов.
Kaspersky Security Network	Миллионы домашних пользователей и тысячи компаний по всему миру добровольно передают в облачную сеть Kaspersky Security Network (KSN) анонимизированные данные о вредоносных программах и подозрительном поведении на своих компьютерах. Этот поток данных, поступающих в режиме реального времени, позволяет нам мгновенно реагировать на появление нового вредоносного ПО и свести к минимуму количество ложных срабатываний.

Функция	Описание
Защита от угроз для мобильных устройств	Защищает мобильные устройства на базе Android и iOS от вирусов и другого вредоносного ПО. Подробнее о функциях для каждой ОС см. ниже.
Интеграция с SIEM-системами	События можно экспортировать в сторонние SIEM-системы, которые обеспечивают безопасность на организационном и техническом уровнях (например в SOC). Позволяет передавать данные по протоколам Syslog и CEF/LEEF.
Интеграция с EMM-системами	Вы можете использовать имеющееся у вас EMM-решение для развертывания и настройки Kaspersky Endpoint Security для Android, совмещая защиту с актуальными бизнес-процессами. Поддерживаемые сторонние EMM: VMware AirWatch, MobileIron, Microsoft Intune, IBM MaaS360 и SOTI MobiControl.

Управление безопасностью

Функция	Описание
Усиление защиты ОС	
Анализ уязвимостей	Предоставляет список установленных на корпоративных устройствах приложений и доступных исправлений для обновления этих приложений до последних версий.
Управление патчами	Позволяет удаленно управлять установкой исправлений и обновлением приложений на корпоративных устройствах. Список приложений доступен в разделе уязвимостей в онлайн-консоли продукта.
Шифрование данных	Позволяет удаленно зашифровать устройства сотрудников с использованием встроенного шифрования Windows (BitLocker) и macOS (FileVault) для защиты корпоративных данных в случае потери или кражи устройства.
Контроль приложений	Управляет запуском программ на компьютерах пользователей и ограничивает доступ к тому или иному ПО, снижая риск заражения. Таким образом можно внедрить корпоративную политику безопасности в отношении использования программ.
Веб-контроль	Позволяет контролировать доступ к интернету в зависимости от типа контента или адреса сайта. Список запрещенных URL-адресов защищает пользователей от посещения потенциально опасных или нежелательных веб-сайтов. Списки доверенных адресов обеспечивают доступ только к безопасным интернет-ресурсам.
Контроль устройств	Контролирует доступ пользователя к внешним и съемным устройствам, подключенным к компьютеру. Администраторы могут разрешить или запретить использование определенных типов устройств или создать список доверенных устройств.
Удаленное уничтожение данных	Позволяет удаленно стереть данные с компьютера пользователя, чтобы защитить их в случае потери или кражи устройства.
Управление мобильными устройствами (MDM)	Позволяет управлять мобильными устройствами сотрудников, применяя к ним политики корпоративной безопасности, контролируя соблюдение требований, защищая устройства от угроз и предотвращая утечку корпоративных данных.

Сценарии использования в IT

Удаленная диагностика клиентских устройств	Защищенные удаленные подключения к рабочему столу или компьютеру клиента позволяют быстро и эффективно устранять неполадки. Механизм авторизации предотвращает несанкционированный удаленный доступ, а все операции, выполняемые во время сеанса удаленного доступа, заносятся в журнал для проверки и аудита. Утилита удаленной диагностики позволяет устранять неполадки в приложениях «Лаборатории Касперского», установленных на управляемых устройствах.
Удаленная установка ОС и приложений	Kaspersky Security Center позволяет создавать образы операционных систем и развертывать их на клиентских устройствах через сеть, а также удаленно устанавливать приложения «Лаборатории Касперского» и других поставщиков программного обеспечения.
Инвентаризация программного и аппаратного обеспечения	Автоматическое обнаружение, а также отслеживание аппаратного и программного обеспечения позволяют администраторам получить полную картину корпоративной сети со всеми устройствами. Автоматизированная проверка ПО позволяет быстро обнаруживать его устаревшие версии, нарушающие безопасность и требующие обновления.

Основные функции EDR

Функция	Описание
Инструменты для расследования и повышения прозрачности	
Карточки обнаружения с анализом первопричин	Общая информация о карточках обнаружения После обнаружения вредоносной или подозрительной активности на устройстве информация о ней автоматически добавляется в карточку обнаружения. Карточка генерируется консолью управления и включает, в частности, следующие данные: • Детальная диаграмма распространения угрозы • Связанные события (зарегистрированные артефакты – сведения о файле или процессе, URL-адрес, изменения реестра и т. д.) • Сведения о хосте (имя, IP-адрес, MAC-адрес, список пользователей, роль контроллера ОС-домена и т. д.) • Общие сведения об обнаружениях, в том числе о режиме детектирования (проверка по требованию, проверка при доступе, AMSI, детектирование при выполнении и т. д.) • Изменение реестра, обнаружения в разделе автозапуска • Статус реагирования (отправлен на карантин, вылечен) • Данные о файле, в том числе: имя и путь, хеш MD5/SHA256, история появления и т. д. Большинство действий по расследованию и реагированию выполняется из карточки обнаружения. Общие сведения об анализе первопричин Этот раздел находится в верхней части карточки оповещения и содержит диаграмму распространения угрозы с ключевыми процессами, сетевыми подключениями, DLL, разделами реестра, которые были затронуты атакой или связаны с оповещением иным образом. Все обнаружения, представленные на диаграмме, выделяются для удобства работы аналитика, который получает полные контекстные данные об инциденте и может быстро найти затронутые компоненты. Диаграмма позволяет получить подробные сведения об инциденте, в том числе дополнительную информацию о процессах и т. д. Все собранные данные, связанные с обнаружением, могут быть отсортированы по группам (процессы, реестр, подключения и т. д.) или связанным спискам.
Аналитические данные об угрозах	Карточки обнаружений содержат данные из глобальной базы знаний «Лаборатории Касперского» об угрозах – это сокращает время и повышает точность анализа первопричин. Вам доступны, в частности, следующие данные: • Статус в Kaspersky Security Network (KSN) • Количество пользователей KSN, которые использовали этот файл • Местоположение пользователей KSN, которые использовали этот файл • Дата первого появления Для получения более подробной информации об обнаруженном файле нужно перейти по встроенной ссылке на портал Kaspersky Threat Intelligence (есть возможность просмотра сведений как в базовой версии, так и в расширенной версии (приобретается отдельно)).
Индикаторы компрометации (IoC)¹	
Реактивный подход	Индикаторы компрометации (IoC), связанные с оповещением или файлом, обнаруженным на диаграмме распространения угрозы, могут генерироваться автоматически, после чего может быть запущен процесс поиска таких индикаторов. Список индикаторов генерируется на основе данных, связанных с соответствующим обнаружением, и передается сотруднику службы безопасности, который принимает решение о последующих действиях, например о поиске аналогичных инцидентов на других хостах или о реализации автоматизированных сценариев реагирования на всех рабочих местах. Список индикаторов компрометации доступен в карточке оповещения. Для поиска аналогичных инцидентов в инфраструктуре используются индикаторы компрометации, автоматически сгенерированные системой. До начала поиска пользователь может выбрать необходимые индикаторы. При поиске по нескольким индикаторам можно задать логические правила обнаружения. Кроме того, можно настроить действия по автоматизированному реагированию, которые будут выполняться при поиске IoC (см. раздел «Реагирование» ниже).

Функция	Описание
Проактивный подход	Использование сторонних индикаторов компрометации в формате OpenIOC упростит работу ИБ-специалистов по поиску IoC. Их можно загрузить в систему, например, из источников, предоставленных поставщиком аналитических данных об угрозах или регулятором, либо с других ресурсов, таких как securelist.ru. Поиск может выполняться в том числе по индикаторам файловых угроз (например, хеш файла). «Лаборатория Касперского» может предоставить список поддерживаемых элементов OpenIOC, чтобы исключить ошибки в синтаксисе IoC и обеспечить их полную поддержку, элементы IoC проверяются при импорте файла (файлов).
Поиск IoC: проверка по расписанию	Поиск IoC в инфраструктуре рабочих мест можно выполнять по расписанию. Он ведется прямо на рабочих местах одновременно с проверкой их статуса.
Экспорт индикаторов компрометации	Автоматически сгенерированные артефакты, связанные с оповещением, можно экспортировать в формате OpenIOC.
Реагирование	
Инструкции по реагированию	Карточка оповещения содержит раздел с рекомендациями по реагированию. Рекомендации представлены в виде пошаговых инструкций с активными ссылками на разделы, где можно выполнить те или иные действия. Таким образом, пользователи могут быстро освоить решение и воспользоваться инструкциями по реагированию при возникновении быстро распространяющейся угрозы.
Реагирование в один клик	Инструменты автоматизированного реагирования позволяют сократить время реагирования с нескольких часов до нескольких минут, а также уменьшить количество рутинных задач, выполняемых вручную. Большинство действий по реагированию можно выполнять всего в несколько кликов прямо из карточки оповещения или детальной диаграммы распространения угрозы. В карточке оповещения есть несколько кнопок, каждая из которых запускает отдельное действие по реагированию: • Запретить запуск файла Объект добавляется в список запрещенных объектов. Это действие можно выполнять на любом участке инфраструктуры рабочих мест. • Изолировать хост Удаленный хост можно изолировать от остальной части сети, чтобы не допустить дальнейшего распространения угрозы. Подключение к консоли управления не разрывается. Пользователь может самостоятельно настроить исключения из этой задачи (добавить в исключения определенные сетевые ресурсы, такие как DNS, или выбрать заранее заданные профили). • Поместить файл на карантин Объект помещается в специальный репозиторий для подозрительных объектов. Файлы, помещенные на карантин, хранятся на защищенном устройстве в зашифрованном виде и не представляют угрозы.
Реагирование через консоль	Для реагирования через консоль вам доступны в том числе следующие действия: • Добавить в список разрешенных объектов Объект добавляется в список разрешенных с помощью доступных в консоли управления инструментов для защиты рабочих мест и управления системами. • Получить файл ИБ-специалист может получить файлы с устройства пользователя. Например, решение можно настроить таким образом, чтобы получать файлы журнала событий, созданные сторонним приложением. Файлы, полученные в результате выполнения этой задачи, будут отправлены на карантин. Загрузить файлы из карантина на свое устройство можно через консоль управления. Расположение файла на устройстве пользователя не меняется. • Удалить файл Объекты можно удалять с одного или нескольких рабочих мест в удаленном режиме. • Запустить процесс На хосте можно удаленно запускать любое дополнительное программное обеспечение. • Завершить процесс Любой подозрительный процесс на рабочем месте можно остановить удаленно, чтобы ограничить распространение угрозы в режиме реального времени и пресечь попытки кражи данных.

¹ Индикаторы компрометации – это следы вредоносной активности, например хеши вредоносных файлов, которые остаются на атакованном устройстве и могут указывать на его заражение или текущую атаку.

Функция	Описание
Автоматическое реагирование на всех рабочих местах на основе индикаторов компрометации	Индикаторы компрометации (IoC), связанные с оповещением или файлом, обнаруженным на диаграмме распространения угрозы, могут генерироваться автоматически, после чего может быть запущен поиск таких индикаторов. Действия по реагированию следующие: • Изолировать хост См. выше • Проверка важных областей Выполняется с помощью инструментов для защиты рабочих мест. • Поместить на Карантин и Удалить файл См. выше
Защита критически важных системных объектов	Если действия по реагированию, такие как Завершить процесс или Удалить файл, запускаются в отношении легитимных и критически важных системных объектов, такие действия блокируются, чтобы не нарушать нормальное функционирование системы.
Восстановление	
Восстановление файла из карантина	Любой объект, находящийся на карантине, может быть восстановлен на рабочем месте в любое время.
Отключение сетевой изоляции	ИБ-специалист может снова подключить изолированные хосты к сети. В правилах изоляции можно настроить тайм-аут автоматического отключения изоляции. Также отключение изоляции может быть выполнено нажатием кнопки в карточке обнаружения после завершения расследования и реагирования.



Поддерживаемые устройства и операционные системы



Windows

[Системные требования](#)



macOS

[Системные требования](#)



Linux

[Системные требования](#)

Мультитенантность

Решения с поддержкой нескольких клиентов используются для защиты инфраструктур сразу нескольких организаций (тенантов).

Они обладают следующими преимуществами.

- Возможность для провайдеров услуг (MS(S)P) защищать несколько клиентов удаленно и без лишних хлопот
- Удобное управление безопасностью в компаниях с географически распределенной инфраструктурой
- Копирование профилей безопасности в рабочих пространствах для быстрого ввода новой тенанты в эксплуатацию

Поставщики MS(S)P, использующие решение Kaspersky EDR для бизнеса Оптимальный, могут предлагать своим клиентам возможности EDR и защиту рабочих мест по модели «как услуга». В Kaspersky EDR для бизнеса Оптимальный могут создаваться независимые тенанты, обеспечивающие дифференциацию данных. Это означает, что данные одного тенанта, например сведения о событиях, оповещениях, пользователях и т. д., недоступны пользователям из другого тенанта. Вместе с тем, у главного администратора (MS(S)P) есть доступ ко всем тенантам, на которых он может запускать процессы обнаружения и реагирования.

Для MS(S)P имеются следующие ключевые возможности.

- **Поддержка нескольких администраторов**
При необходимости решением можно управлять совместно с клиентом.
- **Поддержка нескольких рабочих областей**
В одном окне консоли можно просматривать несколько рабочих областей, что позволяет одновременно работать с несколькими организациями.
- **Совместное управление**
MS(S)P могут подключать внешних администраторов или администраторов компаний-клиентов для совместного управления.
- **Отчетность**
Персонализированные отчеты можно отправлять по расписанию.
- **Гибкая помесечная оплата**
Можно менять количество защищаемых узлов, подключать новых клиентов и платить за максимальное число поддерживаемых узлов в тот или иной месяц.
- **Интеграция** с популярными инструментами удаленного мониторинга и управления (RMM) и автоматизации профессиональных сервисов (PSA).

¹ MSP – поставщик управляемых услуг, MSSP – поставщик управляемых услуг безопасности