Апрель 2022 г.

Список функций Kaspersky Endpoint Security Cloud

kaspersky

kaspersky.ru

Общие сведения

Kaspersky Endpoint Security Cloud (KES Cloud) – решение в рамках модели «Безопасность как услуга» (Security-as-a-Service), которое предназначено для защиты рабочих мест (настольных компьютеров, ноутбуков, файловых серверов и мобильных устройств) на платформах Windows, macOS, Android и iOS и управляется с помощью облачной консоли через браузер.

- Передовые технологии защиты рабочих мест, разработанные ведущим производителем защитных решений
- Простая, интуитивно понятная консоль управления с преднастроенными политиками безопасности
- Облачная консоль для управления безопасностью из любой точки с интернет-доступом

Содержание

Облачная консоль

Бесплатная пробная версия	Вы можете использовать пробную версию Kaspersky Endpoint Security Cloud бесплатно в течение 30 дней. Чтобы продолжить использование продукта после пробного периода, достаточно приобрести лицензию и добавить ее в консоль управления.
Информационная панель для быстрого запуска	Панель информации дает пошаговые инструкции по первоначальной настройке Kaspersky Endpoint Security Cloud. Вы сможете осуществлять мониторинг ваших компьютеров и мобильных устройств, получать статистику Kaspersky Endpoint Security Cloud для вашей компании, а также добавлять или заменять свои лицензии.
Пользовательский интерфейс для IT-администраторов	Полностью обновленная облачная консоль управления максимально упрощает выполнение задач IT-безопасности. Пользовательский интерфейс позволяет IT-администраторам управлять защитой через веб-браузер с любого устройства из любой точки с интернет-доступом.
Kaspersky Business Hub	Неважно, используете ли вы Kaspersky Endpoint Security Cloud или Kaspersky Security для Office 365, вы начинаете работу с продуктом с Kaspersky Business Hub на cloud.kaspersky.com. Kaspersky Business Hub показывает на одном экране все подразделения компании, а поставщикам управляемых услуг – информацию обо всех клиентах. Одна учетная запись дает доступ к нескольким рабочим областям, в том числе для компаний с географически распределенными филиалами. Решение размещается в облаке, поэтому для работы с ним вам понадобятся только веб-браузер и интернет-доступ.
Multi-Tenancy	Решение позволяет поставщикам IT-услуг обеспечивать безопасность клиентов удаленно и без лишних хлопот. Оно также упрощает управление безопасностью в организациях с географически распределенными офисами.
Профили безопасности по умолчанию	Преднастроенные политики, разработанные экспертами «Лаборатории Касперского», обеспечивают мгновенную защиту. Один профиль включает все типы устройств на базе Windows, Windows Server, iOS и Android. Профиль безопасности по умолчанию автоматически применяется к новым устройствам, устраняя необходимость создания политик безопасности для различных устройств вручную. Но при необходимости это легко сделать – решение позволяет создать до 20 профилей для каждой рабочей области.
Профили безопасности пользователей	Профиль безопасности действует для всех устройств конкретного пользователя. Администратору нужно лишь создать профиль, чтобы настройки безопасности были применены ко всем устройствам пользователя под управлением поддерживаемых операционных систем. Для разных групп пользователей можно использовать разные профили в зависимости от выполняемых ими бизнес-задач.
Управление правами администраторов	Если за IT-безопасность в компании отвечают несколько IT-администраторов, можно предоставить им равный доступ к возможностям управления в консоли Kaspersky Endpoint Security Cloud. Это также удобно, если безопасностью управляет сторонняя компания, но сотруднику организации нужен доступ к консоли. ДТП- удалить
Перенос настроек безопасности	Вы можете экспортировать профиль безопасности в файл и перенести настройки безопасности из одного рабочего пространства в другое всего за несколько кликов.

Защита

Многоуровневая защита от вредоносного ПО	Технологии «Лаборатории Касперского» сочетают сигнатурную защиту, эвристический и поведенческий анализ и облачные возможности для защиты рабочих станций Windows от известных, неизвестных и сложных угроз. Использование шаблонов сигнатур позволяет повысить уровень обнаружения вредоносных программ и одновременно уменьшить размер файлов обновлений и освободить каналы связи для других задач.
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 на устройстве опасных скриптов.
Сетевой экран	Сетевой экран защищает каждое конечное устройство 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 предумышленные действия пользователей, нарушающие политику безопасности.
Предотвращение вторжений	Этот компонент 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, такой как вмешательство удаленного устройства в работу операционной системы. При обнаружении попытки сетевой атаки защита от сетевых угроз блокирует сетевую активность, направленную с атакующего компьютера.
Анализ поведения, защита от эксплойтов и откат вредоносных действий	Анализ поведения 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 запуска исполняемого файла уязвимым приложением без участия пользователя этот компонент блокирует исполнение файла. Откат вредоносных действий позволяет отменить действия, выполненные вредоносным ПО в операционной системе, обеспечивая таким образом защиту от шифровальщиков.
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.
Адаптивный контроль аномалий	Этот компонент отслеживает и блокирует операции, нетипичные для компьютеров корпоративной сети. Для выявления подозрительного поведения (например, запуска Microsoft PowerShell из офисного приложения) используется набор правил, разработанный экспертами «Лаборатории Касперского» с учетом типичных сценариев вредоносной активности.
Защита от атак BadUSB	Этот компонент 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.

Расследование и реагирование

Анализ первопричин	Выявляйте и устраняйте скрытые атаки. Анализируйте первопричины, пользуясь визуализацией цепочки атаки. Изучайте подробную информацию для более глубокого анализа.
EDR	Эти технологии автоматически обнаруживают сложные угрозы (в том числе новейшие эксплойты, программы-вымогатели, бесфайловые атаки и атаки с использованием легитимных системных инструментов) и реагируют на них. Варианты действий при обнаружении угрозы: · Поиск индикаторов компрометации · Изоляция хоста · Предотвращение выполнения файла · Отправка файла на карантин · Проверка критичных областей
Тренинги по кибербезопасности для IT-специалистов (CITO)	Встроенные онлайн-тренинги по кибербезопасности помогут IT-специалистам улучшить знания. Модули включают теоретический блок, интерактивные задания в симулированной среде и сертификацию.

Управление безопасностью

Cloud Discovery улучшено	Позволяет обнаруживать и ограничивать несоответствующее или несанкционированное использование облачных ресурсов, а также контролировать рабочее время, проведенное в социальных сетях и мессенджерах. Отслеживает более 1000 облачных сервисов. Мы присвоили рейтинг безопасности известным нам облачным сервисам. С его помощью IT-администраторам легко оценить потенциальные риски, чтобы разрешить или запретить использование конкретного сервиса.
Cloud Blocking	Ограничьте доступ пользователей к нежелательным облачным ресурсам, социальным сетям и мессенджерам.
Data Discovery улучшено	Функция Data Discovery обнаруживает конфиденциальные данные в облаке и определяет, кто имеет к ней доступ. Она обеспечивает прозрачность облачного хранилища и контроль над его содержимым, помогая компаниям предотвращать утечки данных и соблюдать нормативные требования. Data Discovery обнаруживает конфиденциальные данные в SharePoint Online, OneDrive и Teams. Результаты обнаружения отображаются в отчете и специальном списке, а также на виджетах. Типы файлов, которые проходят аудит: doc, docx, ppt, pptx, xls, xlsx, odt, odp, ods, PDF, RTF, jpeg, tiff, png, jp2. Поддерживаемые типы данных: любые номера кредитных карт.
Kaspersky Security для Microsoft Office 365	Расширенные возможности защиты – анти-фишинг, защита от вредоносного ПО, анти-спам, удаление нежелательных вложений и защита по запросу – для всех основных приложений Microsoft Office 365.
Контроль устройств	Контролирует доступ пользователя к внешним и съемным устройствам, подключенным к компьютеру. Администраторы могут разрешить или запретить использование определенных типов устройств или создать белый список доверенных устройств.
Веб-контроль	Позволяет контролировать доступ к интернету в зависимости от типа контента или адреса сайта. Черный список URL-адресов защищает пользователей от посещения потенциально опасных или нежелательных веб-сайтов. Использование белых списков обеспечивает доступ только к безопасным интернет-ресурсам.
Контроль программ	Этот компонент 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.
Анализ уязвимостей	Предоставляет список установленных на корпоративных устройствах приложений и доступных исправлений для обновления этих приложений до последних версий.
Управление установкой исправлений	Вы можете удаленно управлять установкой исправлений и обновлением приложений на корпоративных устройствах. Список приложений доступен в разделе уязвимостей в онлайн-консоли продукта.
Управление шифрованием	Позволяет удаленно зашифровать устройства сотрудников с использованием встроенного шифрования Windows (BitLocker) и macOS (FileVault) для защиты корпоративных данных в случае потери или кражи устройства.
Удаленная очистка данных	Позволяет удаленно стереть данные с компьютера пользователя, чтобы защитить их в случае потери или кражи устройства.

Поддерживаемые устройства и операционные системы

Безопасность и управление для Windows и Windows Server

См. описание приложения

Функция	ПК	Сервер
Защита от файловых угроз	✓	✓
Защита от почтовых угроз	✓	✗
Защита от веб-угроз	✓	✗
Сетевой экран	✓	✓
Защита от сетевых угроз	✓	✓
Анализ поведения	✓	✓
Kaspersky Security Network	✓	✓
Адаптивный контроль аномалий**	✓	✗
Защита от атак BadUSB**	✓	✓
Контроль устройств*	✓	✗
Веб-контроль*	✓	✗
Контроль программ**	✓	✓
Удаленная очистка данных**	✓	✓
Предотвращение вторжений	✓	✗
Cloud Discovery Улучшено	✓	✗
Cloud Blocking*	✓	✗
Управление шифрованием*	✓	✓
Управление установкой исправлений*	✓	✓
Анализ первопричин*	✓	✓
EDR**	✓	✓

Безопасность и управление для Mac OS

См. описание приложения

Функция	Kaspersky Endpoint Security Cloud
Защита от файловых угроз	✓
Защита от веб-угроз	✓
Защита от сетевых угроз	✓
Kaspersky Security Network	✓
Управление шифрованием*	✓

* Функция доступна в Kaspersky Endpoint Security Cloud Plus и Pro
** Функция доступна в Kaspersky Endpoint Security Cloud Pro

Безопасность и управление для Android

См. описание приложения

Функция	Kaspersky Endpoint Security Cloud
Антивирусная защита	✓
Защита паролем	✓
Анти-Вор	✓
Контроль программ	✓
Соответствие политикам	✓
Контроль функций	✓
Веб-контроль	✓
Настройка Wi-Fi	✓
Синхронизация и обновление баз в роуминге	✓

Антивирусная защита
Обнаруживает и нейтрализует угрозы на устройстве с использованием антивирусных баз и облачной базы Kaspersky Security Network. Защищает устройство от вирусов, вредоносных приложений и других угроз в режиме реального времени, проверяет новые приложения и дистрибутивы в папке Загрузки. Проверяет все файлы, которые пользователь открывает, изменяет, перемещает, копирует, запускает или сохраняет на устройстве. Блокирует рекламное ПО и приложения, которые могут быть использованы злоумышленниками с целью повреждения устройства и данных пользователя.

Защита паролем
Защищает доступ к устройству, обеспечивая разблокировку экрана паролем.

Анти-Вор
Защищает информацию, хранящуюся на устройстве, от несанкционированного доступа в случае потери или кражи устройства. Позволяет удаленно заблокировать устройство, включить сирену, определить его местонахождение и стереть на нем данные.

Контроль программ
Использует набор правил для управления программами на пользовательских устройствах. Можно настроить два типа правил: правила для программ и правила для категорий.

Соответствие политикам
Проверяет настройки устройства на соответствие требованиям корпоративной политики безопасности. Например, если устройство было несанкционированно перепрошито или антивирусные базы на нем устарели, можно принять защитные меры.

Контроль функций
Ограничивает доступ пользователя к функциям устройства, включая контроль камеры/Wi-Fi/ Bluetooth.

Веб-контроль
Блокирует доступ к фишинговым и вредоносным веб-сайтам. Ограничивает доступ к веб-сайтам в зависимости от их адреса и типа контента.

Настройка Wi-Fi
Определяет настройки Wi-Fi сети при подключении устройства к интернету.

Синхронизация и обновление баз в роуминге
Выполняет синхронизацию устройства в роуминге с Сервером администрирования. Пользователь также может запустить синхронизацию вручную в любое время. Выполняет обновление антивирусных баз на устройстве в роуминге. Пользователь также может запустить установку обновлений вручную в любое время.

Безопасность и управление для iOS

См. описание приложения

Функция	Kaspersky Endpoint Security Cloud
Веб-контроль	✓
Защита паролем	✓
Настройки прокси-сервера	✓
Анти-Вор	✓
Контроль функций	✓
Настройка Access Point Name	✓
Настройка Air Print	✓
Настройка Wi-Fi	✓
Настройка почты	✓
Настройка CalDAV	✓
Подписка на календари событий	✓

Веб-контроль	Ограничивает доступ к веб-сайтам в зависимости от их адреса и типа контента. Настройки применяются только к supervised devices.
Защита паролем	Защищает доступ к устройству, обеспечивая разблокировку экрана паролем.
Настройки прокси-сервера	Настройки прокси-сервера Защищает трафик при подключении устройства к интернету через глобальный HTTP прокси-сервер. Настройки применяются только к supervised devices.
Анти-Вор	Если устройство украдено, его можно удаленно заблокировать и стереть на нем данные.
Контроль функций	Ограничивает доступ пользователя к встроенным функциям устройства iOS, включая контроль камеры, установку приложений, снятие скриншотов, AirDrop, iCloud и др. Всего поддерживается до 40 различных функций. Обратите внимание, что управление некоторыми функциями возможно только для supervised devices.
Настройка Access Point Name	Настройка Access Point Name (APN) при подключении к службам данных в мобильной сети.
Настройка Air Print	Настройка AirPrint для печати документов с устройства.
Настройка Wi-Fi	Определяет настройки Wi-Fi сети при подключении устройства к интернету.
Настройка почты	Настройка почтовых учетных записей, принадлежащих пользователю устройства.
Настройка CalDAV	Настройка учетных записей CalDAV, принадлежащих пользователю устройства, для работы с календарем событий
Подписка на календари событий	Настройка подписки на чужие календари событий для добавления событий на устройство.

Системные требования

Чтобы управлять Kaspersky Endpoint Security Cloud, нужен только веб-браузер.

Kaspersky Endpoint Security Cloud поддерживает следующие веб-браузеры:

- Microsoft Edge 80 и выше
- Google Chrome 78 и выше
- Mozilla Firefox 72 и выше
- Safari 13 и выше

Kaspersky Endpoint Security Cloud позволяет управлять следующими приложениями «Лаборатории Касперского»:

- Kaspersky Endpoint Security для Windows
- Kaspersky Endpoint Security для Mac
- Kaspersky Endpoint Security для Android
- Устройства iOS, управляемые путем установки сертификатов через сервер iOS Mobile Device Management, размещенный в Kaspersky Endpoint Security Cloud

Kaspersky Endpoint Security Cloud всегда предоставляет последние версии приложений. Они доступны в разделе «Дистрибутивы» консоли управления продуктом.

Полные требования к программному и аппаратному обеспечению доступны в разделе Поддержки в блоке **«Системные требования»** на странице соответствующего приложения «Лаборатории Касперского».

Онлайн-справку по использованию Kaspersky Endpoint Security Cloud можно получить по адресу **https://help.kaspersky.com/Cloud/1.0/ru-RU/123486.htm**

www.kaspersky.ru

kaspersky АКТИВИРУЙ БУДУЩЕЕ