kaspersky

Список функций Kaspersky Security для бизнеса

2024

kaspersky.ru

Общие сведения

Kaspersky Security для бизнеса – это автоматизированная защита рабочих мест от широкого спектра угроз, а также набор важнейших инструментов управления для IT-администраторов в организациях любого размера и из любой отрасли.

Содержание

Введение

Kaspersky Security для бизнеса позволяет управлять следующими приложениями «Лаборатории Касперского»:

- Kaspersky Endpoint Security для Windows
- Kaspersky Endpoint Security для Linux
- Kaspersky Endpoint Security для Mac

Управление приложениями ЛК осуществляется с помощью консоли Kaspersky Security Center (KSC).

Kaspersky Total Security для бизнеса также включает компоненты Kaspersky Security для почтовых серверов и Kaspersky Web Traffic Security. Перейдите по приведенным выше ссылкам, чтобы узнать больше о возможностях этих компонентов.

Актуальная информация и сведения о новых возможностях доступны в соответствующих разделах Онлайн-справки по приложениям «Лаборатории Касперского».

Защита

Защита от файловых угроз	Позволяет избежать заражения файловой системы компьютера. Компонент проверяет файлы на всех дисках компьютера, на подключенных дисках, обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network и эвристического детектирования, включающего анализ как по структурным признакам, так и с помощью эмуляционной песочницы.
Защита от веб-угроз	Предотвращает загрузку вредоносных файлов из интернета, а также блокирует вредоносные и фишинговые веб-сайты. Компонент обеспечивает защиту компьютера с помощью антивирусных баз, облачной службы Kaspersky Security Network и эвристического анализа.
Защита от почтовых угроз	Проверяет вложения входящих и исходящих сообщений электронной почты на наличие в них зловредов и других приложений, представляющих угрозу. По умолчанию данный компонент постоянно находится в оперативной памяти компьютера и проверяет все сообщения, получаемые или отправляемые по протоколам POP3, SMTP, IMAP, NNTP или в почтовом клиенте Microsoft Office Outlook (MAPI).
Сетевой экран	Блокирует несанкционированные подключения к компьютеру во время работы в интернете или локальной сети, контролирует сетевую активность приложений на компьютере. Это помогает защитить компьютеры организации от атак через локальную сеть или, при условии открытого доступа к узлу, через интернет.
Защита от сетевых угроз	Отслеживает во входящем сетевом трафике активность, характерную для сетевых атак. Обнаружив попытку сетевой атаки на компьютер пользователя, приложение блокирует сетевое соединение с атакующим компьютером.
Защита от атак BadUSB	Позволяет предотвратить подключение к компьютеру зараженных USB-устройств, имитирующих клавиатуру.
Защита AMSI	Предназначен для поддержки интерфейса Antimalware Scan Interface (AMSI) от Microsoft. Интерфейс позволяет сторонним приложениям с поддержкой AMSI отправлять объекты (например, скрипты PowerShell) в Kaspersky Endpoint Security для проверки и получать результаты проверки этих объектов.
Предотвращение вторжений	Предотвращает выполнение приложениями опасных действий через ограничение их прав внутри системы, а также обеспечивает контроль доступа к ресурсам операционной системы и персональным данным.
Анализ поведения	Обеспечивает проактивную защиту компьютера. Основываясь на шаблонах опасного поведения и моделях машинного обучения, распознает нежелательную активность внутри системы и блокирует приложения и процессы, инициировавшие эту активность. Позволяет блокировать новейшие образцы вредоносных программ при отсутствии какого-либо предварительного знания о них.
Защита от эксплойтов	Отслеживает и блокирует попытки использования уязвимостей в компонентах ОС и приложениях для исполнения действий, не заложенных в их штатную функциональность; в числе таких действий могут быть загрузка и исполнение зловредных программ, получение привилегий администратора и т.д.
Откат вредоносных действий	Позволяет выполнить откат действий, произведенных вредоносными приложениями в операционной системе. Одним из важнейших сценариев работы данной подсистемы является нивелирование попыток срабатывания программ-шифровальщиков.
Kaspersky Security Network	Инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний «Лаборатории Касперского» о репутации файлов, интернет-ресурсов и программного обеспечения. Использование этих данных обеспечивает более высокую скорость реакции на неизвестные угрозы, повышает эффективность работы компонентов защиты, снижает вероятность ложных срабатываний. Если вы участвуете в Kaspersky Security Network, приложение Kaspersky Endpoint Security получает от служб KSN сведения о категории и репутации проверяемых файлов, а также сведения о репутации проверяемых веб-адресов.

Защита от спама и фишинга на уровне шлюза*	Компонент проверяет сообщения на наличие признаков спама, фишинга и массовых рассылок, в том числе распознает подмену информации в поле FROM и проверяет репутацию IP-адреса посылающего. Фишинг в сообщениях обнаруживается по совокупности признаков; даже самые убедительные фальшивые электронные письма блокируются прежде, чем они попадут на устройство пользователя. Поддержка механизмов аутентификации отправителя дополнительно помогает защитить от компрометации бизнес-переписки, используясь вкупе с другими индикаторами для уменьшения риска ложных срабатываний.
Защита веб-трафика на уровне шлюза*	Компонент обеспечивает безопасность пользователей при использовании веб-ресурсов. В частности, он удаляет вредоносное ПО и другие угрозы из потока данных, поступающего в корпоративную сеть по протоколам HTTP(S) и FTP, блокирует зараженные и фишинговые веб- сайты, контролирует доступ к веб-ресурсам на основе их категорий и типа содержимого и обеспечивает фильтрацию трафика для снижения рисков заражения и потери ценных данных.

* Эти функции доступны в рамках лицензий Kaspersky Total Security и Total Security Plus для бизнеса.

Шифрование данных

Шифрование файлов	Позволяет создавать правила шифрования файлов. Есть возможность выбрать для шифрования стандартные папки, выбрать папку вручную или выбрать отдельные файлы по расширению.
Полнодисковое шифрование	Позволяет зашифровать диск с помощью следующих технологий: Шифрование диска Kaspersky или Шифрование диска BitLocker.
Шифрование съемных дисков	Позволяет защитить данные на съемных дисках. Есть возможность использовать следующие виды шифрования: полнодисковое шифрование (FDE) и шифрование файлов (FLE).

Задачи по обеспечению безопасности

Поиск вредоносного ПО	Выполняет проверку компьютера на присутствие вирусов и других приложений, представляющих угрозу. Позволяет исключить возможность распространения вредоносных приложений, которые не были обнаружены другими компонентами.
Откат последнего обновления	Отменяет последнее обновление баз и модулей. Это позволяет вернуться к использованию предыдущих баз и модулей приложения при необходимости, например, в том случае, если новая версия баз содержит некорректную сигнатуру, из-за которой Kaspersky Endpoint Security блокирует безопасное приложение.
Проверка целостности	Проверяет модули приложения, находящиеся в папке установки приложения, на наличие повреждений или изменений. Если модуль приложения имеет некорректную цифровую подпись, то такой модуль считается поврежденным.
Поиск индикаторов компрометации (IoC)	Позволяет запускать задачи по поиску индикаторов компрометации вручную* или в автоматизированном** режиме и выполнять действия по реагированию на угрозы.
Запуск/завершение процесса	Позволяет удаленно запускать файлы и завершать их работу.

* Функция доступна в рамках лицензии Kaspersky Endpoint Security для бизнеса Стандартный и выше.
** Функция доступна в рамках лицензии Kaspersky EDR для бизнеса Оптимальный.

Контроль безопасности

Контроль приложений	Управляет запуском приложений на компьютерах пользователей. Это позволяет выполнить политику безопасности организации при использовании приложений. Контроль приложений снижает риск заражения компьютера, ограничивая доступ к приложениям.
Контроль устройств	Управляет доступом пользователей к установленным или подключенным к компьютеру устройствам (например, жестким дискам, камере или модулю Wi-Fi). Это позволяет защитить компьютер от заражения при подключении этих устройств и предотвратить потерю или утечку данных.
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.
Адаптивный контроль аномалий*	Отслеживает и блокирует действия, нехарактерные для компьютеров сети организации с помощью набора правил, созданных специалистами «Лаборатории Касперского» на основе типичных сценариев вредоносной активности. Вы можете выбрать поведение Адаптивного контроля аномалий для каждого из правил. Kaspersky Endpoint Security обновляет набор правил с базами приложения.
Анализ журналов	Контролирует целостность защищаемой среды на основе результатов анализа журналов событий Windows. При обнаружении признаков нетипичного поведения в системе приложение информирует администратора, так как это поведение может указывать на попытки кибератак.
Мониторинг файловых операций	Обнаруживает изменения объектов (файлов и папок) в заданной области мониторинга. Эти изменения могут указывать на нарушение безопасности компьютера. При обнаружении изменения объектов приложение информирует администратора.

* Компонент доступен в рамках лицензий Kaspersky Endpoint Security для бизнеса Расширенный и выше.

Detection and Response

Endpoint Detection and Response Optimum*	Защищает IT-инфраструктуру организации от сложных киберугроз, в том числе новых эксплойтов, программ-вымогателей, бесфайловых атак (фишинг), а также схемв с применением легитимных системных утилит. Функциональность решения сочетает автоматизированное обнаружение угроз с возможностью реагирования на них.
Endpoint Detection and Response Expert*	Предлагает пользователю больше функций для мониторинга и реагирования на угрозы информационной безопасности, чем EDR Optimum.
Kaspersky Sandbox**	Обнаруживает и автоматически блокирует сложные угрозы на компьютерах, анализирует поведение объектов для выявления вредоносной активности и признаков целевых атак на IT-инфраструктуру. Выполняет анализ и проверку объектов на специальных серверах с развернутыми виртуальными образами операционных систем Microsoft Windows.
Managed Detection and Response*	Обнаруживает и анализирует инциденты безопасности в вашей инфраструктуре. Для этого MDR использует данные телеметрии, полученные от конечных точек, и передовые технологии. Данные об инцидентах MDR передает экспертам «Лаборатории Касперского». Далее эксперты могут самостоятельно обработать инцидент и, например, добавить новую запись в антивирусные базы. Также эксперты могут дать рекомендации по обработке инцидента и, например, предложить изолировать компьютер от сети.

* Отдельная лицензия.
** Компонент доступен в рамках лицензии Kaspersky Total Security Plus для бизнеса

Консоль управления

Kaspersky Security для бизнеса обеспечивает гибкие возможности управления через Kaspersky Security Center (KSC). Вы можете управлять безопасностью через локальную или облачную[1] консоль. Для управления через облако вам не придется развертывать сервер управления и привлекать ресурсы для его обновления – об этом позаботится «Лаборатория Касперского».

Если вы предпочитаете установить сервер управления внутри корпоративного периметра или работаете с изолированными средами, вы можете использовать:

- Веб-консоль Kaspersky Security Center, которая позволяет создавать и обслуживать систему безопасности через веб-интерфейс.
- Консоль администрирования, которая реализована для KSC Windows на основе Microsoft Management Console (MMC);

Используя Kaspersky Security для бизнеса с помощью Kaspersky Security Center, вы можете:

- Формировать иерархию Серверов администрирования для снижения нагрузки на Серверы администрирования и внутреннего трафика (что особенно полезно для удаленных офисов), а также для распределения обязанностей между ИБ-администраторами.
- Управлять доступом на основе ролей для создания пользовательских учетных записей и ролей и управления ими.
- Выполнять отказоустойчивую кластеризацию для повышения доступности Kaspersky Security Center и снижения времени простоя Сервера администрирования в случае сбоя.
- Создавать иерархию групп администрирования для управления выбором клиентских устройств в целом.
- Выполнять удаленную установку приложений «Лаборатории Касперского» и других поставщиков программного обеспечения.
- Удаленно управлять приложениями «Лаборатории Касперского» и других поставщиков, установленными на клиентских устройствах.
- Получать уведомления о критических событиях, возникших во время работы приложений «Лаборатории Касперского».
- Управлять шифрованием информации, хранящейся на жестких дисках устройств и съемных накопителях, а также доступом пользователей к зашифрованным данным.
- Выполнять централизованное развертывание лицензионных ключей для приложений «Лаборатории Касперского» на клиентских устройствах, отслеживать их использование и продлевать лицензии.
- Устанавливать обновления и устранять уязвимости[2]
- Получать статистические данные и отчеты о работе управляемых программных продуктов и устройств, а также отчеты о состоянии системы безопасности.

[1] Подробнее: https://support.kaspersky.com/KSC/CloudConsole/ru-RU/195507.htm

[2] На Linux посредством задачи удаленной установки

Возможности по администрированию

Управлением устройствами	Позволяет управлять устройствами сотрудников на базе операционных систем Windows, Linux,MacOS
Установка приложений*	Позволяет удаленно устанавливать приложения «Лаборатории Касперского» и других поставщиков ПО.
Учет программного и аппаратного обеспечения*	Автоматическое обнаружение, а также отслеживание аппаратного и программного обеспечения позволяют администраторам получать полную картину корпоративной сети со всеми устройствами. Автоматизированная проверка приложений позволяет быстро обнаруживать их устаревшие версии, создающие риски и требующие обновления.
Управление доступом на основе ролей*	Позволяет настраивать права доступа к функциям приложения для отдельных пользователей и групп пользователей Kaspersky Security Center, а также создавать стандартные пользовательские роли с заранее определенными правами на основе должностных обязанностей.
Удаленное устранение неполадок	Защищенное удаленное подключение к компьютеру клиента позволяет устранять неполадки быстро и эффективно. Механизм авторизации предотвращает несанкционированный удаленный доступ, а все операции, выполненные в ходе сеанса, заносятся в журнал для проверки и аудита. Утилита удаленной диагностики позволяет устранять неполадки в приложениях «Лаборатории Касперского», установленных на управляемых устройствах.
Проверка на уязвимости	Позволяет осуществлять учет установленных на корпоративных устройствах приложений и анализ доступных исправлений для обновления данных приложений до последних версий
Управление установкой исправлений*	Позволяет удаленно управлять установкой исправлений и обновлением приложений на корпоративных устройствах. Список приложений доступен в разделе уязвимостей в онлайн-консоли решения.
Обновление	Позволяет загружать обновленные базы, модули приложения и ретранслировать их управляемым продуктам для обновления. Это обеспечивает актуальность защиты компьютера от вирусов и других приложений, представляющих угрозу. По умолчанию приложение обновляется автоматически, но при необходимости вы можете вручную обновить базы и модули приложения.
Установка операционных систем*	Позволяет создавать образы операционных систем и развертывать их на клиентских устройствах по сети.
Интеграция с SIEM-системами	Позволяет экспортировать события в сторонние SIEM-системы, которые обеспечивают безопасность на организационном и техническом уровнях (например, в SOC). Некоторые лицензии позволяют передавать данные по протоколам Syslog и CEF/LEEF.

* Компонент доступен в рамках лицензий Kaspersky Endpoint Security для бизнеса Расширенный и выше.

Сравнение доступных возможностей разных методов управления

Функция или возможность	Kaspersky Security Center в инфраструктуре клиента		Kaspersky Security Center в облаке
	Windows	Linux	
Расположение Сервера администрирования	Локально	Локально	Облачная среда
Расположение системы управления базами данных (СУБД)	Локально	Локально	Облачная среда
Тип консоли администрирования	Локальная и веб-интерфейс	Веб-интерфейс	Веб-интерфейс
Обслуживание Сервера администрирования и СУБД	Ответственность клиента	Ответственность клиента	Ответственность «Лаборатории Касперского»
Иерархия Серверов администрирования	✓	✓	✓ (Может использоваться только в качестве главного Сервера администрирования в иерархии)
Иерархия групп администрирования	✓	✓	✓
Миграция управляемых устройств и связанных с ними объектов из локальной версии Kaspersky Security Center в облачную	✓	✗	✓
Опрос сети	✓	✓ (только по IP-диапазонам)	✓ (только по точкам распространения)
Максимальное количество управляемых устройств	100 000	20 000	25 000
Защита управляемых устройств на базе Windows, Linux и macOS	✓	✓	✓
Политики приложений «Лаборатории Касперского»	✓	✗	✓
Задачи для приложений «Лаборатории Касперского»	✓	✓	✓
Kaspersky Security Network	✓	✓	✓
Прокси-сервер KSN	✓	✓	✓ (только на точках распространения)
Kaspersky Private Security Network	✓	✓	✗
Централизованное развертывание лицензионных ключей для приложений «Лаборатории Касперского»	✓	✓	✓
Перенос управляемых устройств на другой Сервер администрирования	✓	✓	✗ (для переноса управляемых устройств на другой Сервер администрирования на них нужно переустановить Агент администрирования)
Поддержка виртуальных Серверов администрирования	✓	✓	✓
Установка обновлений для стороннего ПО и устранение уязвимостей в сторонних программах	✓	✗	✓ (устанавливаются только рекомендуемые исправления)
Уведомления о событиях на управляемых устройствах	✓	✓	✓
Управление шифрованием	✓	✓	✓ (только BitLocker)
Создание пользовательских учетных записей и управление ими	✓	✓	✓
Максимальное количество событий в базе данных	Зависит от размера развернутой БД	Зависит от размера развернутой БД	400 000 (зависит от количества управляемых устройств)
Использование Сервера администрирования в качестве сервера WSUS	✓	✗	✗
Мониторинг статусов политик и задач	✓	✓	✓
Поддержка кластеров и массивов серверов в группах администрирования	✓ (только в консоли администрирования MMC)	✗	✗

Рабочие станции и серверы на базе Windows. Безопасность/управление

См. описание приложения

Поддерживаемые ОС для рабочих станций:

- ✓ Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 или выше
- ✓ Windows 8 Professional / Enterprise
- ✓ Windows 8.1 Professional / Enterprise
- ✓ Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise
- ✓ Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise

Поддерживаемые серверные ОС:

- ✓ Windows MultiPoint Server 2011 (64-разрядная)
- ✓ Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 или выше
- ✓ Windows Server 2012 Foundation / Essentials / Standard / Datacenter
- ✓ Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter
- ✓ Windows Server 2016 Essentials / Standard / Datacenter
- ✓ Windows Server 2019 Essentials / Standard / Datacenter
- ✓ Windows Server 2022

Поддерживаемые типы терминальных серверов:

- ✓ Службы удаленных рабочих столов Microsoft на базе Windows Server 2008 R2 SP1/ 2012/2012 R2/2016/2019

Функция	Рабочая станция	Сервер
Защита от файловых угроз	✓	✓
Защита от веб-угроз	✓	✓
Защита от почтовых угроз	✓	✓
Сетевой экран	✓	✓
Защита от сетевых угроз	✓	✓
Защита от атак BadUSB	✓	✓
Защита AMSI	✓	✓
Предотвращение вторжений	✓	✓
Анализ поведения	✓	✓
Защита от эксплойтов	✓	✓
Откат вредоносных действий	✓	✓
Kaspersky Security Network	✓	✓
Адаптивный контроль аномалий	✓	
Полное шифрование диска*	✓	
Шифрование дисков BitLocker*	✓	✓
Шифрование файлов*	✓	
Шифрование съемных дисков*	✓	
Контроль приложений	✓	✓
Веб-Контроль	✓	✓
Контроль устройств	✓	✓
Адаптивный контроль аномалий	✓	
Анализ журналов		✓
Мониторинг файловых операций	✓	✓
Управление шифрованием*	✓	✓
Интеграция с SIEM-системами	✓	✓
Установка операционных систем и приложений	✓	✓
Учет программного и аппаратного обеспечения	✓	✓
Инвентаризация	✓	✓
Удаленная очистка данных	✓	✓
Удаленное устранение неполадок	✓	✓
Поиск вредоносного ПО	✓	✓
Проверка на уязвимости	✓	✓
Управление установкой исправлений	✓	✓
Обновление баз	✓	✓
Откат последнего обновления	✓	✓
Проверка целостности	✓	✓
Интеграция с EDR	✓	✓
Интеграция с MDR	✓	✓

* Компонент доступен в рамках лицензий Kaspersky Endpoint Security для бизнеса Расширенный и выше.

macOS
Безопасность/управление

См. описание приложения

Поддерживаемые ОС для рабочих станций:
- ✓ macOS 10.14–12 Поддержка Intel и Apple Silicon

Функция	
Защита от файловых угроз	✓
Защита от веб-угроз	✓
Защита от сетевых угроз	✓
Проверка на наличие вирусов и других вредоносных программ	✓
Обновление баз	✓
Резервное хранилище	✓
Отчеты о работе программы	✓
Уведомления о событиях	✓
Центр защиты	✓
Удаленное управление программой через Kaspersky Security Center	✓
Шифрование дисков*	✓
Веб-Контроль	✓
Интеграция с MDR	✓

* Компонент доступен в рамках лицензий Kaspersky Endpoint Security для бизнеса Расширенный и выше.

Linux
Безопасность/управление

См. описание приложения

Поддерживаемые ОС для рабочих станций:
- ✓ Red Hat Enterprise Linux 6.7/7.2/8.0 и выше
- ✓ Ubuntu 18.04 LTS / 20.04 LTS и выше
- ✓ CentOS 6.7/7.2/8.0 и выше
- ✓ Debian GNU Linux 9.4/10.1/11.1 и выше
- ✓ Mageia 4 AlmaLinux 8.4/8.5 AlterOS 7.5 и выше
- ✓ Amazon Linux 2 Astra Linux Common Edition (обновление 2.12); Astra Linux Special Edition RUSB.10015-01 (обновление 1.5/1.6); Astra Linux Special Edition RUSB.10015-16 (выпуск 1) (обновление 1.6)
- ✓ EulerOS V2.0SP2 2.2.17/ SP5 2.5.6 Linux Mint 19/ 20.1 и выше
- ✓ openSUSE Leap 15.0 и выше
- ✓ Oracle Linux 7.3/8.0 и выше
- ✓ Pardus OS 19.1 SUSE Linux Enterprise Server 12 SP5/ 15 и выше
- ✓ Альт Образование / Рабочая станция / Сервер 9 Goslinux 7.2 RED OS 7.3

Функция	
Защита от файловых угроз	✓
Защита от сетевых угроз	✓
Сетевой экран	✓
Защита от веб-угроз	✓
Kaspersky Security Network	✓
Анализ поведения	✓
Контроль программ*	✓
Контроль устройств	✓
Защита от шифрования[1]	✓
Проверка важных областей[2]	✓
Инвентаризация программного обеспечения	✓
Контроль целостности**	✓
Интеграция с MDR	✓
Защита контейнеров***	✓

* Компонент доступен в рамках лицензий Kaspersky Endpoint Security для бизнеса Расширенный и выше.

** Доступно в лицензиях Kaspersky Security для систем хранения данных и лицензии Enterprise решения Kaspersky Security для виртуальных и облачных сред

*** Ограниченно доступен во всех уровнях Kaspersky Security для бизнеса, полная функциональность - как в **

[1] Защита файлов, передаваемых по протоколам SMB/NFS, от вредоносного шифрования
[2] Объектов автозапуска, загрузочных секторов, памяти процессов и ядра

Новости о киберугрозах: www.securelist.ru
Новости IT-безопасности: business.kaspersky.ru

www.kaspersky.ru

kaspersky активируй будущее

© 2024 АО «ЛАБОРАТОРИЯ КАСПЕРСКОГО». ЗАРЕГИСТРИРОВАННЫЕ ТОВАРНЫЕ ЗНАКИ И ЗНАКИ ОБСЛУЖИВАНИЯ ЯВЛЯЮТСЯ СОБСТВЕННОСТЬЮ ИХ ПРАВООБЛАДАТЕЛЕЙ.