Kaspersky® Security для бизнеса

Контроль рабочих мест

Мощные инструменты контроля рабочих мест, тесно интегрированные с передовыми технологиями защиты от вредоносных программ помогают защитить ваш бизнес от современных динамично развивающихся угроз.

Защита, применение политик, контроль

Уязвимости в доверенных приложениях, вредоносные веб-ресурсы и недостаточно эффективный контроль периферийных устройств в условиях постоянного появления все более сложных угроз – вот лишь некоторые проблемы, с которыми сталкиваются современные компании. Контроль программ, Веб-контроль и Контроль устройств – это разработанные «Лабораторией Касперского» эффективные инструменты, которые позволяют обеспечить полный контроль рабочих мест в составе корпоративной сети, не снижая при этом ее производительность.

Контроль программ и динамические белые списки

Решение «Лаборатории Касперского» обеспечивает надежную защиту от известных и новых угроз, позволяя IT-администраторам полностью контролировать работу приложений, разрешенных к использованию на рабочих местах, вне зависимости от действий сотрудника. Мониторинг активности программ оценивает поведение приложений и эффективно блокирует любые нежелательные действия, которые могут поставить под угрозу безопасность рабочего места и корпоративной сети в целом.

- **Контроль запуска программ** – разрешает, блокирует и ведет учет запуска программ. Позволяет повысить эффективность работы сотрудников за счет ограничения запуска приложений, не имеющих прямого отношения к рабочему процессу.
- **Мониторинг уязвимостей** – проактивная защита от атак, использующих уязвимости в доверенных приложениях.
- **Контроль активности программ** – регулирует и контролирует доступ приложений к ресурсам системы и данным. Распределяет программы по следующим категориям: доверенные, слабо ограниченные, сильно ограниченные и недоверенные. Управляет доступом программ к зашифрованным данным –например, к информации, передаваемой через веб-браузеры или Skype™.

В большинстве защитных решений других производителей средства контроля обеспечивают только базовый функционал блокирования/разрешения доступа. В отличие от них, средства контроля «Лаборатории Касперского» используют облачные белые списки, позволяющие оперативно получать доступ к самой актуальной информации о приложениях.

Технологии контроля программ, разработанные «Лабораторией Касперского», используют облачные белые списки для анализа и мониторинга программы на каждой стадии – при ее загрузке, установке и запуске.

Технология динамических белых списков, используемая в политике «Запрет по умолчанию», блокирует попытки запуска на рабочем месте любых программ, за исключением разрешенных администраторами. «Лаборатория Касперского» – единственная в отрасли IT-безопасности компания со специализированной Whitelisting-лабораторией, которая осуществляет постоянный мониторинг и обновление базы белых списков, содержащей более 500 миллионов программ.

Политика «Запрет по умолчанию» может применяться в тестовой среде, позволяя администраторам определять легитимность программ до их блокирования. Также возможно создание категорий программ на основе цифровых подписей, чтобы предотвратить запуск легитимного ПО, было изменено вредоносными программами или получено из подозрительного источника.

Веб-контроль

Мониторинг, фильтрация и контроль веб-сайтов, на которые пользователь может заходить со своего рабочего места, позволяют повысить производительность труда и при этом обеспечить защиту от веб-угроз и вредоносных атак. «Лаборатория Касперского» создала и постоянно обновляет базу веб-сайтов, сгруппированных по категориям (сайты «для взрослых», игры, социальные сети, азартные игры и т.д.). Администраторы могут легко создавать и применять политики, которые запрещают, ограничивают или отслеживают доступ конечных пользователей к отдельным сайтам или категориям сайтов, а также создавать собственные списки сайтов. Доступ к вредоносным сайтам блокируется автоматически.

Ограничивая использование социальных сетей и служб мгновенного обмена сообщениями, Веб-Контроль помогает предотвратить утечку данных. Гибкие политики позволяют разрешать сотрудникам просмотр веб-сайтов в определенные часы.

Для усиления защиты Веб-Контроль работает непосредственно на компьютере пользователя. Благодаря этому любая заданная политика продолжает применяться, даже когда пользователь находится вне периметра корпоративной сети.

Простое управление

Инструменты контроля рабочих мест интегрируются с Active Directory, что упрощает создание и быстрое применение комплексных политик в масштабах организации. Управление всем функционалом осуществляется через единую консоль с помощью единого интерфейса.

Контроль устройств

Для эффективного решения проблем, связанных с использованием съемных устройств, недостаточно просто отключить USB-порт. Помимо прочего, это может затронуть другие меры защиты, такие как применение USB-токена для организации VPN-доступа к корпоративной сети.

Контроль устройств обеспечивает более гибкий контроль на уровне шины, типа устройств и отдельных устройств, предоставляя оптимальную защиту без замедления работы пользователя. Политики контроля могут также применяться в зависимости от серийного номера устройства.

- Устанавливает правила подключения/чтения/записи для различных устройств с возможностью применения политик по расписанию.
- Задает правила контроля устройств на основе масок, устраняя необходимость физического подключения устройств для занесения их в белые списки. Позволяет одновременно заносить в белые списки группы устройств.
- Контролирует обмен данными через съемные устройства внутри и за пределами организации, снижая риск потери или кражи данных.
- Интегрируется с технологиями шифрования «Лаборатории Касперского» для внедрения политик шифрования на заданных типах устройств.

www.kaspersky.ru

#ИстиннаяБезопасность

Как приобрести

Инструменты контроля рабочих мест не продаются отдельно. Они доступны в следующих продуктах линейки Kaspersky Security для бизнеса:

- Kaspersky Endpoint Security для бизнеса Стандартный
- Kaspersky Endpoint Security для бизнеса Расширенный
- Kaspersky Total Security для бизнеса

Кроме того, инструменты контроля устройств и веб-контроля доступны в решении Kaspersky Endpoint Security Cloud