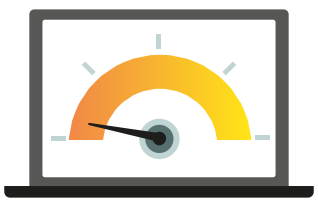
Экономьте ресурсы с Kaspersky Endpoint Security Cloud

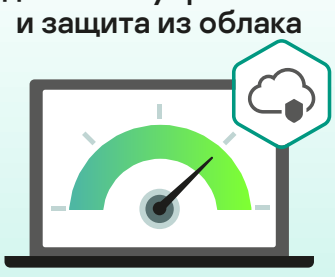
Частый сценарий

Защитное ПО
без централизованного управления



Kaspersky Endpoint Security Cloud

Удаленное управление
и защита из облака



Развертывание защитного приложения

В каждый компьютер нужно вставить USB-флешку, чтобы установить приложение

Затем добавляется лицензия

Далее для агента задаются параметры подключения к консоли управления

Благодаря облачной консоли управлять установкой и настройкой защиты можно когда и откуда угодно

Достаточно указать адреса электронной почты всех сотрудников, чтобы отправить им ссылку на установку приложения

Готово! Остальное произойдет автоматически

Создание политики безопасности

Политика создается с нуля

В лучшем случае мастер создания политики попросит вас выбрать множество параметров, часть из которых вы видите впервые

Политика по умолчанию будет применена ко всем устройствам автоматически

При желании вы можете изменить настройки позже и создать различные профили на основе политики по умолчанию

Обнаружение теневых IT

Приходится подключаться к роутеру или отслеживать трафик вручную с помощью анализатора

Нужно приобрести дорогостоящее решение класса CASB[1] и подключить его к IT-инфраструктуре

Достаточно открыть специальный виджет в консоли управления и за несколько кликов:

1. Получить отчет об использовании теневых IT
2. Заблокировать часть сервисов/пользователей и создать исключения для VIP-пользователей

Защита Microsoft Office 365 от фишинга и вредоносного ПО

Компании используют встроенную защиту в надежде, что она справится с угрозами

Приобретается дорогостоящая служба Microsoft ATP

Приобретается стороннее решение для защиты электронной почты и облака

В состав Kaspersky Endpoint Security Cloud Plus входит защита для основных приложений, включая Exchange Online, OneDrive, SharePoint Online и Teams

Управление установкой исправлений

Исправления устанавливаются вручную, либо приобретается специальное ПО

Встает выбор: оставить уязвимости в системе или раздражать коллег установкой исправлений в их рабочее время

Остается один выход: устанавливать исправления после работы, жертвуя отдыхом

Можно запланировать автоматическую установку исправлений в нерабочее время

Не жертвовать рабочим и личным временем, чтобы установить исправления

Антивирусные проверки

Приходится ставить напоминания, чтобы не забыть обновить базы и запустить проверку всех компьютеровв офисе

Annoy users with lowering computers performance during scans

Нет необходимости запускать проверку вручную

Kaspersky Endpoint Security Cloud незаметно проверяет компьютеры, когда они не используются, не мешая пользователям

Полное шифрование диска

Встроенного в ОС шифрования достаточно, если все сотрудники находятся в одном офисе

Для эффективной работы BitLocker нужна локальная папка Active Directory. Этот вариант не подходит для удаленных сотрудников

Шифровать устройства можно удаленно прямо из консоли Kaspersky Endpoint Security Cloud с использованием встроенных средств ОС (BitLocker в Windows и FileVault в macOS)

[1] Cloud Access Security Broker
(брокер безопасного доступа к облаку)

kaspersky