



Безопасность мобильных устройств

«Лаборатория Касперского» объединила технологии защиты от мобильных угроз и управления ими (MTD и MTM), чтобы сотрудники компаний могли использовать для работы мобильные устройства, не подвергая риску конфиденциальные бизнес-данные и критически важные процессы. Мы предлагаем передовую защиту от вредоносного ПО и спама, веб-контроль, контроль устройств и приложений для Android и iOS, а также защиту от кражи.

Ниже описаны возможности защиты и управления для мобильных устройств, используемых на работе.

Мобильные угрозы становятся всё сложнее

За всю свою историю «Лаборатория Касперского» выявила **более 40 миллионов мобильных угроз**.

В ходе нашего исследования бизнеса в 2019 году:

- более **40%** опрошенных рассказали о **ненадлежащей передаче корпоративных данных с помощью мобильных устройств** в их компаниях;
- в **16%** таких случаев произошла **утечка данных**.

Почему так важна защита мобильных устройств?

Большинство людей сейчас сильно зависят от мобильных устройств как на работе, так и в личной жизни, и границы между этими сферами размыты. Тем временем мобильные угрозы становятся все сложнее. Устройства Android особенно уязвимы, хотя устройства iOS в этом их быстро догоняют.

Именно поэтому безопасность мобильных устройств не менее важна, чем защита ноутбуков и компьютеров. Сотрудники организаций часто работают удаленно и используют мобильные устройства не только для личного, но и для делового общения.

Как «Лаборатория Касперского» защищает мобильные устройства?

Мы предлагаем комплексную защиту мобильных устройств, в том числе принадлежащих сотрудникам (BYOD), в рамках комплексных решений для защиты и контроля рабочих мест – [Kaspersky Endpoint Security Cloud](#) и [Kaspersky Security для бизнеса](#).

Защита мобильных устройств с учетом бизнес-требований

В Kaspersky Endpoint Security Cloud предусмотрена защита двух мобильных устройств на пользователя – рабочее и личное устройства каждого сотрудника будут в безопасности. Клиенты из SMB-сегмента получают надежную защиту данных и устройств сотрудников без лишних затрат.

Kaspersky Security для бизнеса не только выявляет и блокирует мобильные угрозы, но также гибко подстраивается под требования конкретной организации и легко интегрируется с существующей инфраструктурой и инструментами, например с решениями для управления мобильными устройствами (EMM). Безопасность мобильных устройств включена во все уровни Kaspersky Security для бизнеса.

Решения класса EMM, с которыми интегрируются наши технологии

- Microsoft Intune
- VMware AirWatch
- MobileIron
- IBM Maas360
- SOTI MobiControl
- Другие EMM-платформы для конфигурирования приложений

Интеграция с EMM

Средства обнаружения мобильных угроз, доступные в Kaspersky Security для бизнеса, интегрируются с современными платформами класса EMM.

Список функций для защиты мобильных устройств и управления ими

Защита и управление для Android		
	Kaspersky Endpoint Security Cloud	Kaspersky Security для бизнеса
Развертывание/обновление:	✓	✓
с помощью Google Play	✓	✓
с помощью отдельных установочных пакетов	✗	✓
с помощью сторонних EMM-решений	✗	✓
Защита от вредоносного ПО с облачной аналитикой	✓	✓
Компонент Анти-Вор	✓	✓
Аутентификация с помощью пин-кода / отпечатка пальца	✓	✓
Удаленные команды обнаружения/блокирования/очистки	✓	✓
Соответствие нормативам	✓	✓
Обнаружение root-прав на устройстве	✓	✓
Соответствие требованиям, установленным для разных типов устройств	✓	✓
Контроль приложений	✓	✓
Контроль камеры / Wi-Fi / Bluetooth	✓	✓
Веб-Контроль и защита от онлайн-угроз	✗	✓
Предоставление сертификатов электронной почты / безопасного соединения	✗	✓
Android Enterprise / Exchange ActiveSync	✗	✓
Конфигурирование приложений с помощью сторонних EMM-платформ	✗	✓
Безопасность и управление для iOS		
Веб-защита	✗	✓
Компонент Анти-Вор (блокирование и очистка)	✓	✓
Создание профилей iOS MDM	Не требуется	Силами клиента
Сервер iOS MDM	✓	✓
Аутентификация с помощью пин-кода / Face ID / Touch ID	✓	✓
Настройка прокси-сервера	✓	✓
Фильтрация веб-контента	✓	✓
Настройка Wi-Fi	✓	✓
Управление ограничениями для приложений и встроенными функциями iOS	✓	✓
Настройка AirPlay/AirPrint	✓	✓
Настройка электронной почты/календаря/контактов	✓	✓
Ограничения для медиаконтента	✗	✓
Предоставление сертификатов электронной почты / безопасного соединения	✗	✓

Лицензирование защиты для мобильных устройств

Мы стремимся обеспечить максимально гибкое лицензирование для предприятий любого масштаба.

Каждая пользовательская лицензия Kaspersky Endpoint Security Cloud включает защиту двух мобильных устройств, чтобы можно было безопасно использовать личное и служебное устройство.

Лицензию Kaspersky Security для бизнеса можно применить к любому устройству: настольному компьютеру, серверу, мобильному устройству. Такая прозрачная модель лицензирования позволяет защищать множество рабочих мест, не уточняя количество устройств каждого типа, – достаточно знать только общее число защищаемых устройств.