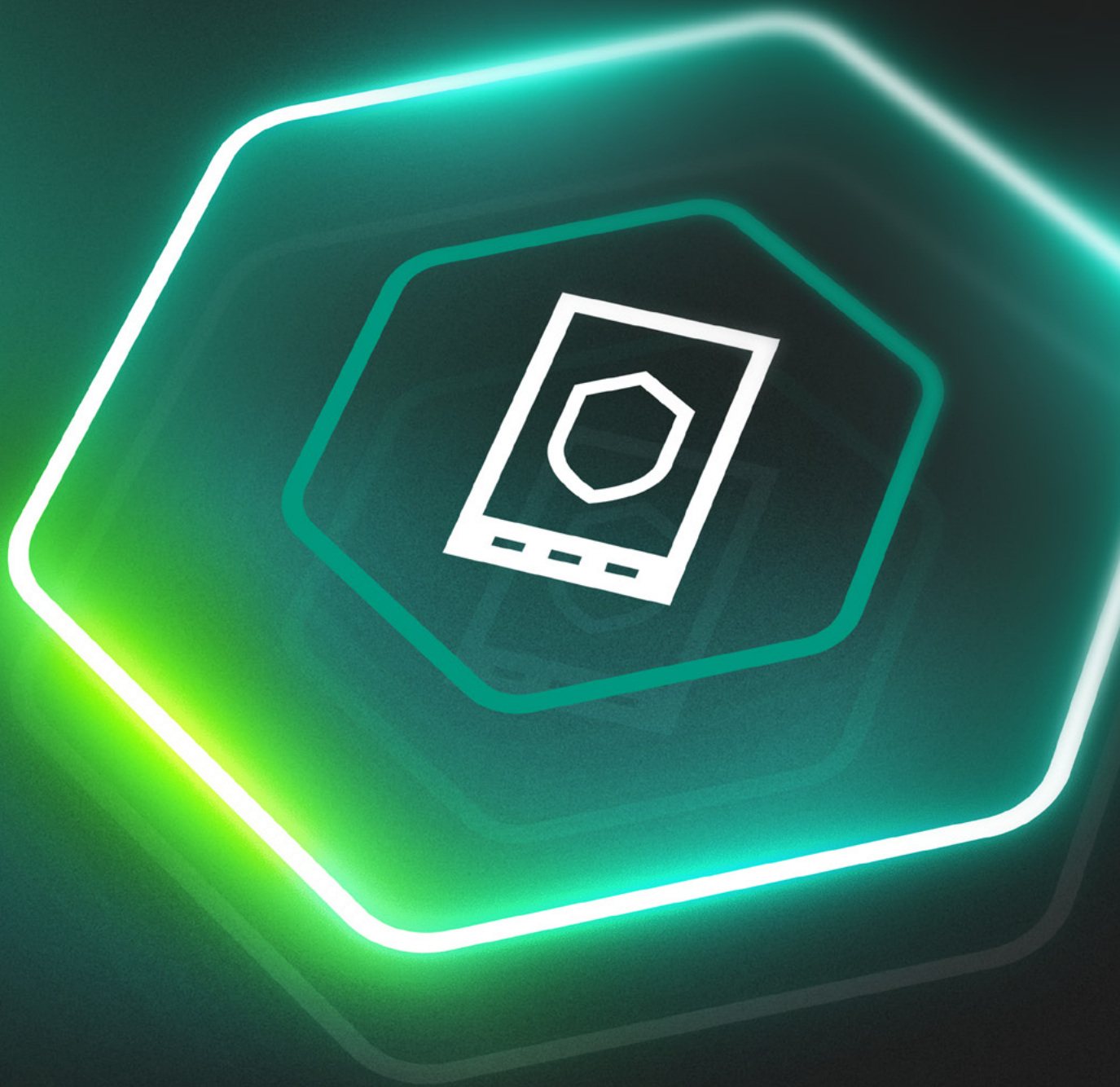




Безопасное, гибкое и удобное
управление мобильными
ресурсами компании

Kaspersky Secure Mobility Management

kaspersky

АКТИВИРУЙ
БУДУЩЕЕ

Актуальные реалии и риски для компаний

- Разветвленная и распределенная ИТ-инфраструктура современных организаций
- Широкое использование смартфонов (корпоративных и личных) для работы
- Популярность BYOD-подхода
- Распространение удаленного и гибридного формата работы
- Цифровая трансформация бизнеса
- Рост таргетированных кибератак на компании, в т. ч. через мобильные устройства

Безопасное, гибкое и удобное управление мобильными ресурсами компании

Мобильность — необходимое качество для успешного бизнеса сегодня. Чтобы контролировать парк мобильных устройств и обеспечить их безопасное использование, необходимо применять решения, которые учитывают их специфику, — это касается и установки приложений, и доступа к корпоративным ресурсам, и защиты от угроз.

Kaspersky Secure Mobility Management — надежное российское решение, предназначенное для удаленного управления мобильностью предприятия: мобильными устройствами, процессами, данными и их безопасностью.

Ключевые преимущества

Полная поддержка жизненного цикла

Одно из ключевых отличий мобильных устройств от стационарных компьютеров — более динамичный жизненный цикл. Такие устройства не только сталкиваются с дополнительными рисками безопасности, но и чаще переходят из рук в руки, выводятся из употребления, заменяются на новые. Kaspersky Secure Mobility Management поддерживает все этапы этого цикла.

Признанные технологии защиты

«Лаборатория Касперского» постоянно исследует угрозы и интегрирует эти знания в разработку продуктов, поэтому решение обеспечивает высокий уровень безопасности для корпоративных мобильных устройств.

Органический элемент защитной экосистемы

Для большинства компаний защита ИТ-инфраструктуры с помощью решений «Лаборатории Касперского» давно стала стандартом. Kaspersky Secure Mobility Management построен на основе проверенных принципов и рабочих процессов, а значит его освоение и использование не потребует дополнительных усилий.

Жизненный цикл использования корпоративных мобильных устройств

Подготовка

Развертывание сервисов поддержки мобильной платформы (серверная часть)

Подготовка корпоративного каталога со списком доверенных приложений и портала для подключения BYOD-устройств

Подготовка и конфигурирование сценариев автоматизированного развертывания корпоративных устройств

Поддержка и выводение из обслуживания

Обеспечение удаленной поддержки

Аудит потерянных / украденных устройств

Отзыв доступа к корпоративным ресурсам

Выборочное (для BYOD-устройств) или полное обнуление (очистка) устройства

Развертывание и конфигурация

Загрузка сертификатов безопасности, профилей email, VPN, Wi-Fi

Установка агентской части решения, обеспечивающей защиту устройств и функции мониторинга/контроля

Загрузка и применение корпоративных политик безопасности и ограничений использования

Установка и автоматизированное конфигурирование бизнес-приложений

Защита и контроль

Отслеживание событий безопасности

Реагирование на события уровня «инцидент», включающее вмешательство администратора

Отслеживание и реагирование на события регуляторных политик

Ключевые возможности



Управление и поддержка сценариев работы

Автоматизированное управление жизненным циклом

Решение позволяет заранее сконфигурировать сценарии работы (Device Owner, киоск, Supervised, или BYOD), доступы к ресурсам (установка сертификатов), профили работы нужных приложений и их доступность в корпоративном каталоге. Устройство может быть подготовлено к работе столь же быстро, как и выведено из эксплуатации при утере или краже.

Прозрачность инфраструктуры и интеграция

Управление и мониторинг осуществляется из единой точки — консоли Kaspersky Security Center, что позволяет контролировать и унифицированно управлять другими защитными решениями.

Широкий спектр поддерживаемых устройств

Решение обладает функциональностью таких классов, как MDM, EMM и UEM. Оно открывает широкие возможности управления устройствами на базе распространенных мобильных ОС и позволяет автоматизировать операции, связанные с жизненным циклом рабочих станций под управлением Windows.



Защита

Защита от вредоносных программ

Проверяйте программы при установке, сканируйте по требованию и/или расписанию. Непрерывная защита в реальном времени обеспечивает надежную защиту от зловредных и нежелательных программ.

Защита от веб-угроз

Рабочие устройства защищены от атак из интернета, таких как фишинговые веб-сайты или точки распространения зловредного ПО.

Антифишинг

Применение социальной инженерии с целью привлечь пользователя на зловредные интернет ресурсы будет заблокировано вне зависимости от канала применения, будь то почта, СМС или социальные сети.



Контроль

Максимальное сокращение рисков

Вы контролируете список веб-ресурсов, приложений и периферии, которые можно использовать на устройстве, уменьшая риски заражения и потери данных.

Контроль над функциональностью системы

Использование памяти устройства, сетевые взаимодействия, наличие привилегированного доступа, геопозиция и многое другое регулируются политиками компании — владельца устройств. В случае нарушения правил использования и срабатывания других критериев, будут автоматически применены действия, которые предотвратят возникновение инцидента.

Управление доступом к ресурсам и соблюдение требований регуляторов

Решение поддерживает категоризацию веб-ресурсов, включающую не только опасные, но и потенциально нежелательные интернет-ресурсы, а также списки ограничений, накладываемых федеральными законами о защите данных и требованиями регуляторов. Это позволяет дополнительно снижать риски потери ценных данных и нарушения требований регулирующих органов.

> 1,5 млн

вредоносных установочных пакетов для мобильных устройств обнаружила «Лаборатория Касперского» по всему миру в 2022 году

> 101 млн

уникальных вредоносных веб-ссылок потенциально угрожающих мобильным устройствам

> 109 млн

количество уникальных вредоносных объектов

Премиальная поддержка и профессиональные сервисы

Специалисты технической поддержки готовы прийти на помощь в любой момент. Воспользуйтесь премиальными пакетами [Расширенной технической поддержки](#) или [профессиональными сервисами](#). Они помогут извлечь максимум из установленных у вас решений «Лаборатории Касперского», обеспечивая быструю установку и бесперебойное функционирование вашей инфраструктуры ИТ-безопасности.

Построение экосистемы безопасности с «Лабораторией Касперского»

Kaspersky Secure Mobility Management дополняет богатую экосистему решений «Лаборатории Касперского» для всесторонней защиты бизнеса от киберугроз. В ее основе — более чем 25-летний опыт работы на глобальных рынках и технологии, признанные независимым экспертным сообществом, международными аналитическими агентствами и пользователями со всего мира.

Современные компании стремятся комплексно подходить к защите инфраструктуры. Использование Kaspersky Secure Mobility Management способствует развитию этого подхода, позволяя включить мобильные устройства в экосистему кросс-продуктового детектирования и реагирования — XDR.

Решения, которые дополняют Kaspersky Secure Mobility Management:



Kaspersky Security для виртуальных и облачных сред

Передовые технологии защиты и соответствие нормативным требованиям для виртуальных и облачных рабочих нагрузок, контейнеров и VDI.



Kaspersky Security для почтовых серверов

Защита нового поколения от угроз, связанных с электронной перепиской.



Kaspersky Security Awareness

Тренинги в игровом формате помогают развить навыки кибергигиены у сотрудников и сформировать культуру кибербезопасного поведения в организации.



Kaspersky Secure Mobility Management

[Подробнее](#)

www.kaspersky.ru

© 2023 АО «Лаборатория Касперского».
Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

#kaspersky
#активируйбудущее