Check Point
SOFTWARE TECHNOLOGIES LTD.

Harmony
Mobile

HARMONY MOBILE: ЗАЩИТА МОБИЛЬНЫХ УСТРОЙСТВ ОТ КИБЕРУГРОЗ

3 млрд

телефонов оказались подвержены уязвимостям Achilles, которые дают полный контроль над устройством (Check Point, июль 2020)

1700 приложений

с вредоносным программным обеспечением Joker были обнаружены и удалены из Google Play в феврале 2020 года

в **2** раза

выросло количество вредоносных программ, которые обнаруживаются в магазине приложений Google Play за год (по данным 2020 г.)

#1

Harmony Mobile был признан самым эффективной защитой мобильных устройств от известных и новых угроз (Miercom, 2019)

Смартфоны – неотъемлемая часть рабочего пространства

Смартфоны уже давно стали полноценной частью рабочей среды сотрудника. Электронная почта и календарь, сервисы обмена сообщениями, доступ к рабочим ресурсам и корпоративным приложениям, видео-конференции, – все эти инструменты делают сотрудников более мобильными и эффективными.

К сожалению, преимуществами дело не ограничивается. Злоумышленники давно поняли, что информация на мобильном телефоне зачастую даже более полезна и конфиденциальна, чем та, что хранится на рабочем компьютере, а заполучить ее проще. Установив контроль над телефоном, хакер получает не только доступ к корпоративным ресурсам и сервисам, но и возможность развивать свою атаку, используя социальную инженерию.

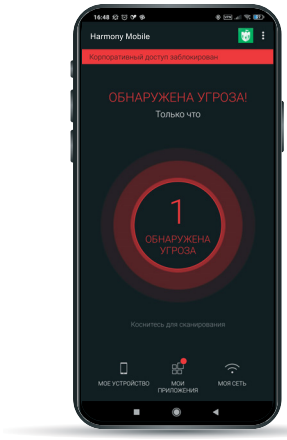
Когда пользователи получают доступ к рабочим ресурсам с мобильных устройств, важнейшей задачей становятся мониторинг и обеспечение безопасности этих устройств, а также хранимых на них корпоративных данных.

Если дело касается мобильных телефонов, особенно личных, пользователи зачастую более беспечны: они устанавливают приложения, которые им нравятся, легче подвержены социальной инженерии и фишингу. Обеспечивая их защиту, важно соблюсти баланс между приватностью и необходимыми ограничениями.

Как хакеры атакуют телефоны

Приложения

Каждый год Google удаляет из официального магазина тысячи вредоносных приложений, загруженных миллионы раз. Многие пользователи готовы загружать «бесплатные» версии платных приложений из сторонних источников. Зачастую телефоны малоизвестных брендов поставляются с уже предустановленными приложениями, которые содержат вредоносный код или критические уязвимости.



Фишинг

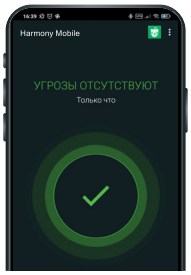
Фишинг на мобильных телефонах становится мейнстримом. Существует множество способов доставки фишинговых сообщений: от SMS и различных мессенджеров до почты.

Уязвимости и ошибки конфигурации ОС

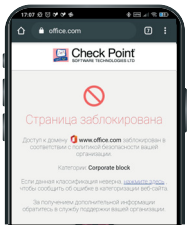
Каждый год количество уязвимостей, обнаруживаемых в iOS и Android, растет, а их эксплуатация может дать хакеру полный контроль над устройством.

Harmony Mobile – необходимая защита для устройства

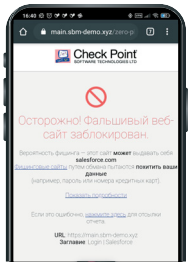
Защита от вредоносного ПО
- проверка списка приложений
- обнаружение известных и новых угроз
- статический и динамический анализ (эмуляция), анализ исходного кода
- инспекция приложений из сторонних источников
- блокировка опасных сайтов и серверов
- техники и тактики по матрице MITRE ATT&CK



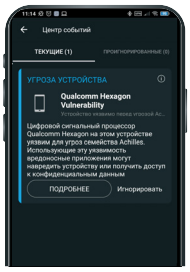
Условный доступ
- ограничение доступа к корпоративным ресурсам (например, к Office365) с атакованных или уязвимых устройств
- URL-фильтрация
- ограничение доступа к корпоративным данным на устройстве (с помощью MDM)



Антифишинг
- блокировка известных и новых фишинговых сайтов
- инспекция содержимого веб-страниц с помощью машинного обучения
- работа с любым браузером и любым мессенджером
- предотвращение утечки паролей



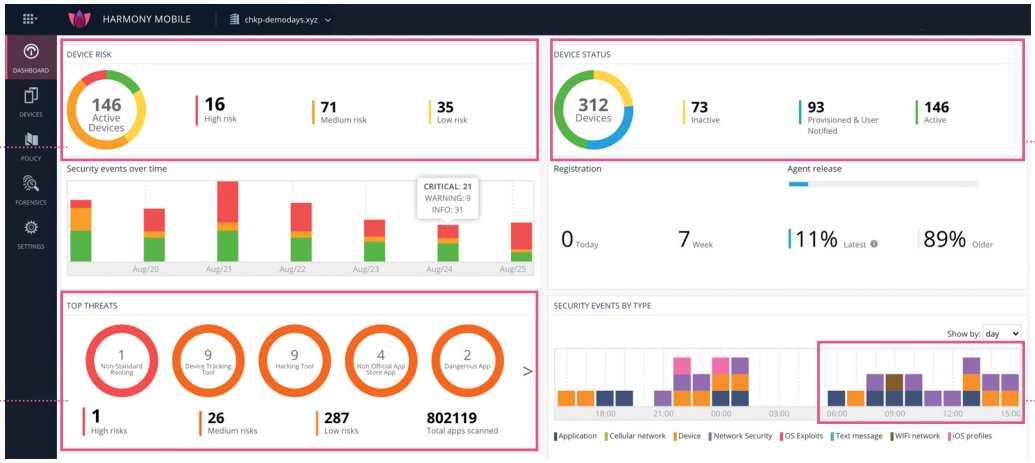
Защита от уязвимостей и проверка конфигурации
- уязвимые версии приложений и самой ОС
- вредоносные профили прокси и VPN
- сторонние сертификаты
- опасные настройки устройства



Полный контроль безопасности

Риски

Наиболее критичные угрозы



Статус развертывания

Инциденты за последнее время

Преимущества интеграции с MDM/UEM

Решения MDM/UEM предназначены для управления устройствами и не способны защитить от вредоносных приложений, фишинга и других атак. Однако, наличие платформы управления дает Harmony Mobile преимущества, например, централизованное развертывание и дополнительные возможности по предотвращению атак.

CITRIX · Enterprise Mobility Suite · vmware Workspace™ ONE™ · MobileIron · BlackBerry UEM · jamf · IBM MaaS360 | With Watson · android enterprise recommended · Check Point Capsule

#1 Решение Harmony Mobile признано лидером своего сегмента в независимых тестах и исследованиях рынка Mobile Threat Defense

Gartner · Miercom · IDC Analyze the Future

Представительство в России и СНГ
Check Point Software Technologies (Russia) ООО
109544, Москва, бульвар Энтузиастов, 2, Деловой центр «Голден Гейт»
Тел./факс: +7 495 967 7444 • www.checkpoint.com/ru • Эл. почта: Russia@checkpoint.com