СПЕЦИФИКАЦИЯ

Symantec Endpoint Protection Mobile (Skycure Mobile Threat Defense)

Умная защита для умных устройств

Почему SEP Mobile?

Комплексная безопасность
Многоуровневая защита мобильных устройств от известных, неизвестных и целенаправленных угроз по всем векторам атаки.

Предиктивная технология
Выявление и блокировка подозрительных сетей, разработчиков и приложений до того, как они могли бы причинить вред.

Незаметность и производительность
Общедоступное мобильное приложение помогает защитить устройство, не оказывая негативного влияния на удобство использования и скорость разряда аккумулятора.

Простая установка
Приложения для iOS и Android быстро устанавливаются, легко обслуживаются и поддерживаются.

Корпоративный масштаб
Автоматическое соблюдение ИТ-политик за счет интеграции с имеющимися EMM/ MDM, почтовыми серверами и VPN. SEP Mobile можно установить на тысячах устройств за считанные минуты.[1]

Эффективность и наглядность
Превосходная наглядность информации о мобильных уязвимостях, угрозах и атаках; автоматическое обнаружение и удаление.

Мощный коллективный анализ
Защита от атак «нулевого дня» с помощью компетентного и эффективного сообщества экспертов по безопасности мобильных устройств.

Огромный опыт в кибербезопасности
Сотрудники SEP Mobile Research Labs обладают огромным опытом поиска и исследования новых уязвимостей и угроз. В каждой из последних четырех версий iOS нами была обнаружена и исправлена по крайней мере одна уязвимость.

Обзор решения

Symantec Endpoint Protection Mobile (SEP Mobile) представляет собой комплексное, высокоточное и эффективное решение для защиты мобильных устройств. Непревзойденная глубина анализа позволяет предсказывать и выявлять множество известных и неизвестных угроз. В предиктивной технологии SEP Mobile применен многоуровневый подход, включающий в себя коллективное исследование угроз, анализ на устройстве и на сервере. Такой подход позволяет превентивно защищать мобильные устройства от вредоносных программ, сетевых угроз, использования уязвимостей приложений и ОС как при наличии подключения к Интернету, так и оффлайн.

Компоненты решения

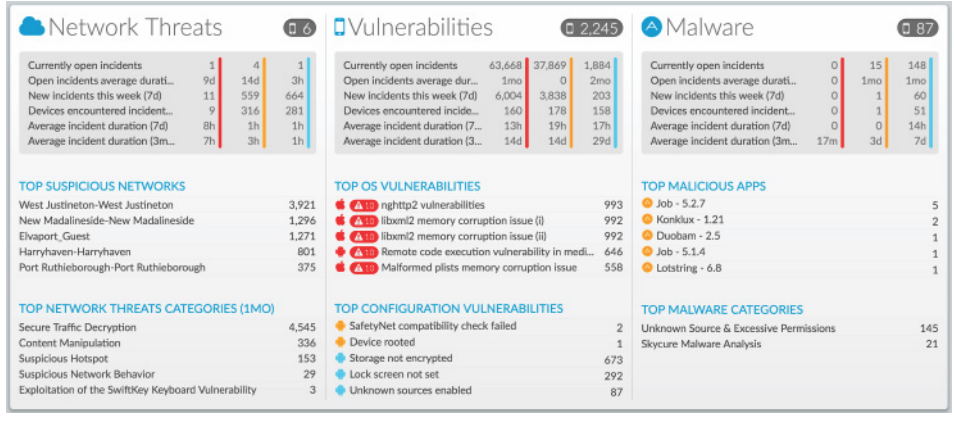
Корпоративная платформа SEP Mobile состоит из следующих компонентов:

Мобильное приложение

- Простота установки, внедрения, обслуживания и обновления
- Не влияет[2] на производительность, удобство и конфиденциальность
- Защита от подозрительных приложений и сетей в реальном времени
- Автоматическая защита корпоративных ресурсов во время атаки
- Обмен данными с коллективной системой исследования угроз SEP Mobile

Облачные серверы

- Глубокий вторичный анализ подозрительных приложений
- Анализ репутации с машинным обучением: приложения, сети и ОС
- Обширная база данных коллективного анализа угроз
- Применение политик за счет интеграции с EMM, VPN, Exchange и другими системами
- Подробные журналы активности для интеграции с любым решением класса SIEM



[1] По данным об установке у заказчиков

[2] По отзывам заказчиков

Широкий фронт защиты

Защита от вредоносных программ

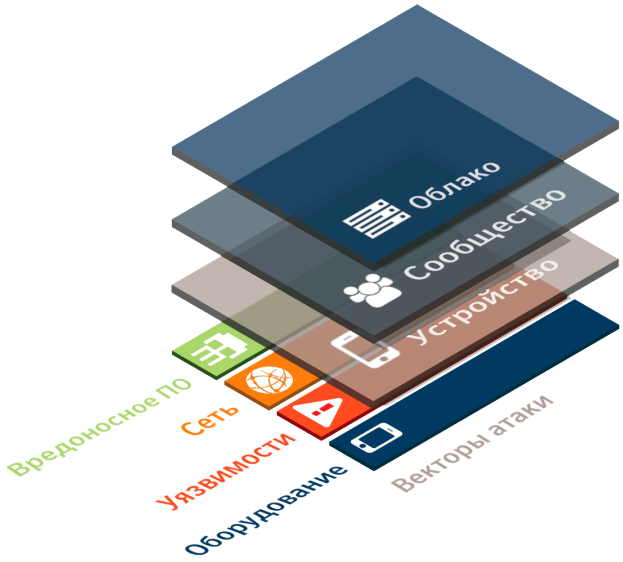
- Превентивная защита от вредоносных переупакованных приложений, использующих уязвимости «нулевого дня».
- Инкрементальное исследование приложений с использованием сигнатуры, статического и динамического анализа, поведения, структуры, запрашиваемых разрешений, источника и других факторов.
- Реагирование и защита в реальном времени от известных, неизвестных и целенаправленных атак.

Защита от угроз из сети

- Эффективное экранирование вредоносных сетей Wi-Fi.
- Обнаружение, блокирование и удаление вредоносных профилей iOS.
- Запатентованная технология «активной приманки» для обнаружения атак Man-in-the-Middle, SSL Downgrade и манипулирования содержимым.

Защита от уязвимостей

- Мониторинг известных незакрытых уязвимостей на устройствах.
- Обучение пользователей и уведомление ИТ-персонала.
- Выявление уязвимостей «нулевого дня» в приложениях и операционных системах, уведомление разработчиков.
- Обнаружение неизвестных и известных уязвимостей, таких как Stagefright и Accessibility Clickjacking.



Физическая защита

- Единственное решение MTD со встроенными функциями MDM и возможностью интеграции с имеющимися решениями EMM/MDM.
- Удаленное стирание в случае кражи или компрометации устройства.
- Защита корпоративной информации паролем.
- Автоматическое обновление приложений SEP Mobile и профилей.
- Подробные отчеты об устройствах, пользователях и группах.

Глубокий анализ

Облачный сервер

- Специалисты SEP Mobile Research Labs мыслят как хакеры, чтобы всегда опережать их.
- Глубокий статический и динамический анализ, включая поведенческий анализ с использованием машинного обучения.
- Постоянный мониторинг и оценка рисков, связанных с открытыми уязвимостями.
- Получение аналитики от других корпоративных систем (EMM, SIEM).

Коллективный разум

- Каждое устройство с SEP Mobile работает как датчик и накопитель данных.
- Поддерживается каталог характеристик «хороших» и «плохих» приложений и сетей.
- Оценивается возможность исправления новых версий ОС и типов устройств.
- Самый эффективный способ выявления уязвимостей «нулевого дня» — переупакованных приложений и других вредоносных программ.

Устройство

- Первая линия обороны, выявление подозрительных приложений и сетей.
- Инкрементальный анализ приложений по множеству характеристик.
- Мгновенная идентификация безопасных и подозрительных сетей.
- Оценка рисков на основании типа устройства, версии ОС и других характеристик.

Бесплатная пробная версия*

Узнайте, каким угрозам подвержена ваша организация, с помощью пробной версии и оценки рисков. Это займет не больше 5 минут. **Воспользуйтесь бесплатной пробной версией** ➤

*** Действуют определенные условия и ограничения**

Symantec™ + Skycure®

350 Ellis St., Mountain View, CA 94043 США
1 (800) 650 4821 | hello@skycure.com | www.symantec.com

SYMC-DS-Skycure-v5