Введение

На данный момент, существует огромное количество разновидностей вредоносного ПО для совершения различных атак и нанесения ущерба цифровому пространству. Поэтому для защиты информации люди придумали защитное ПО. Сейчас в мире существует множество различных компаний, занимающиеся исследованиями и разработкой программ. Некоторые делают ПО для целевой защиты от конкретного вредоносного элемента, другие – создают комплексную защиту и выпускают её на рынок, как полноценный программный продукт.

Основная часть

Symantec Endpoint Protection (SEP) — пакет программного обеспечения для организации безопасности, который включает функции защиты от вредоносных программ, предотвращения вторжений и брандмауэра для серверов и настольных компьютеров. У него самая большая доля рынка среди продуктов для защиты конечных точек. SEP разработан компанией Broadcom Inc.

Согласно SC Magazine, Symantec Endpoint Protection также имеет некоторые функции, типичные для программного обеспечения для предотвращения потери данных. Обычно он устанавливается на сервере под управлением Windows, Linux или macOS. По состоянию на 2018 год, версия 14 является единственной поддерживаемой версией.

Symantec Endpoint Protection сканирует компьютеры на наличие угроз безопасности. Используется для предотвращения запуска неутвержденных программ, и для применения политик брандмауэра, которые блокируют или разрешают сетевой трафик. Пытается идентифицировать и блокировать вредоносный трафик в корпоративной сети или исходящий из веб-браузера. Использует совокупную информацию от пользователей для выявления вредоносного ПО. По состоянию на 2016 год Symantec утверждает, что использует данные со 175 миллионов устройств, на которых установлена Symantec Endpoint Security, в 175 странах.

Symantec Endpoint Protection имеет административную консоль, которая позволяет ИТ-отделу изменять политики безопасности для каждого отдела, например, какие

программы или файлы следует исключить из антивирусного сканирования. Он не управляет мобильными устройствами напрямую, но рассматривает их как периферийные устройства при подключении к компьютеру и защищает компьютер от любого вредоносного программного обеспечения на мобильном устройстве.

По данным Gartner, Symantec Endpoint Protection 14 является одним из наиболее полных доступных продуктов для обеспечения безопасности конечных точек и регулярно получает высокие баллы в независимых тестах.

Network World поставила Symantec Endpoint Protection на шестое место среди продуктов для обеспечения безопасности конечных точек на основе данных тестирования NSS Labs.

Заключение

Symantec Endpoint Protection является зарекомендовавшим себя решением для корпоративных сетей, дата-центров и прочей информационной инфраструктуры. Не смотря на критику, связанную с изменчивостью в направлении развития продукта данное решение продолжает набирать высокие рейтинги.

Данное решение использует передовые технологии и подходы, соответствующие времени. Версия 14 включает технологию машинного обучения для поиска закономерностей в цифровых данных, которые могут указывать на наличие угрозы кибербезопасности.