DATA SHEET

FireEye

Система безопасности конечных точек FireEye Endpoint Security

Построена экспертами для защиты конечных точек от значимых угроз

КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА

- Развертывание в локальных, облачных или виртуальных средах вместе с агентом конечной точки для обнаружения, предотвращения и контроля активности локальных или удаленных конечных точек
- Полностью интегрированный рабочий процесс проверки и анализа с единым агентом конечных точек, объединяющий анализ угроз, анализ поведения и обнаружение, предотвращение и исправление вредоносных программ
- Обеспечивает подробное исследование конечных точек с полной хронологией активности в рамках одного рабочего процесса, чтобы персонал мог быстро идентифицировать и сдержать инверсии управления (IOCs) и другие угрозы или подозрительную активность
- Поиск, обнаружение и сдерживание угроз на десятках тысяч конечных точек (подключенных или нет) за минуты
- Единый интерфейс для легкой оценки всей активности конечных точек, выявления и анализа инцидентов и сдерживания их одним щелчком мыши для исключения риска заражения

Традиционная защита конечных точек оставляет пробелы в своих попытках устранить современные угрозы. Система безопасности конечных точек FireEye Endpoint Security улучшает обозримость безопасности, а также качество и релевантность угроз вашим данным для устранения этих пробелов и дает вам:

- Полностью интегрированную защиту от вредоносных программ (защита от вирусов (AV)), исправление, анализ поведения, оперативные данные и видимость конечных точек
- Встроенный обозреватель сортировки и аудита Triage and Audit Viewer для проведения исчерпывающей проверки и анализа индикаторов угрозы
- Поисковик безопасности предприятия Enterprise Security Search для быстрого нахождения и освещения намерения подозрительной деятельности или угрозы
- Сбор данных для проведения детальной глубокой проверки и анализа конечных точек в течение определенного периода времени
- Защита от инструментов эксплуатации уязвимости Exploit Guard для обнаружения, предупреждения и предотвращения атак, нацеленных на нецелевое использование или эксплуатацию приложения.

Объединение обнаружения и ответа конечных точек (EDR) и других возможностей в единое интегрированное решение FireEye предоставляет аналитикам самый быстрый способ проверки, поиска и анализа любой подозрительной активности на любой конечной точке, что позволяет им адаптировать защиту на основе подробной информации об угрозе в реальном времени.

Обнаружение и предотвращение скрытых процессов использования конечных точек

Когда дело доходит до обнаружения и предотвращения использования, традиционные возможности защиты конечных точек ограничены, поскольку инструменты эксплуатации уязвимости не соответствуют простой подписи или шаблону. Система безопасности конечных точек FireEye Endpoint Security предоставляет гибкий, управляемый данными об инструментах эксплуатации уязвимости поведенческий интеллект через функцию Exploit Guard (защита от инструментов эксплуатации уязвимости). Эта функция также работает с Endpoint Detection and Response (EDR) (обнаружение и ответ конечных точек) с подробной информацией, которую традиционные решения конечных точек пропускают, с помощью FireEyeexclusive для соотнесения множественных дискретных действий для выявления активности инструмента эксплуатации уязвимости.

Распространение информации об угрозах на каждую конечную точку
Для обеспечения эффективности на точке атаки должна присутствовать оперативная информация об угрозе. Возможности обнаружения и ответа конечных точек (EDR), предлагаемые системой безопасности конечных точек Endpoint Security, беспрепятственно расширяют возможности передачи оперативной информации об угрозах других продуктов FireEye на конечную точку. Если какой-либо продукт FireEye обнаруживает атаку в любом месте сети, конечные точки автоматически обновляются, и аналитик может быстро проверить и собрать подробные данные об инверсиях управления (IOCs) с помощью обозревателя сортировки и аудита Triage and Audit Viewer на каждой конечной точке.

Достижение лучшей видимости конечных точек
Полная видимость конечных точек имеет решающее значение для выявления основной причины оповещения и проведения глубокого анализа угрозы для определения ее состояния. Ретроспектива кэширования в системе безопасности конечных точек Endpoint Security позволяет вам проверять и анализировать настоящие и прошлые оповещения на любой конечной точке для тщательного экспертного исследования и лучшего реагирования.

Получите полное покрытие конечной точки с помощью защиты от вредоносных программ
Обеспечивает всестороннюю защиту всех конечных точек с помощью агента защиты от несанкционированного доступа, а также сканирование доступа в режиме реального времени ко всем типам файлов с использованием подписи, эвристики, общего обнаружения и эмуляции (“песочница”) и сканирования по запросу (по расписанию) полной, оперативной памяти, основной загрузочной записи (MBR) и загрузочной записи тома (VBR).

Сдерживание скомпрометированных конечных точек и предотвращение бокового распространения
Атаки, начинающиеся в конечной точке, могут быстро распространиться по вашей сети. После того, как вы идентифицируете атаку, система безопасности конечных точек Endpoint Security позволяет сразу изолировать скомпрометированные устройства одним щелчком мыши, чтобы остановить атаку и предотвратить ее распространение в боковом направлении или чтобы она не стала представлять собой большую угрозу другим способом. Затем вы можете провести полное экспертное исследование инцидента без риска дальнейшего заражения и принять меры по исправлению на основе подробного исследования и анализа действия угрозы.

Как работает система безопасности конечных точек
Система безопасности конечных точек Endpoint Security может осуществлять поиск и исследовать известные и неизвестные угрозы на десятках тысяч конечных точек за минуты. Она использует динамические оперативные данные об угрозах FireEye Dynamic Threat Intelligence для соотнесения оповещений, генерируемых FireEye, и продуктов сетевой безопасности и журналов безопасности для подтверждения достоверности угрозы:

- Идентифицируйте и детализируйте векторы атаки, используемые для просачивания в конечную точку
- Определите, произошла ли (и сохраняется ли) атака на определенной конечной точке
- Проверьте, произошло ли боковое распространение и на какие конечные точки
- Установите временные рамки и как долго была скомпрометирована конечная точка (точки)
- Отследите инцидент, чтобы определить, просочилась ли наружу интеллектуальная собственность, и какая она
- Четко определите, какие конечные точки и системы нуждаются в сдерживании для предотвращения дальнейшей компрометации.

Требования системы безопасности конечных точек
Для системы безопасности конечных точек необходим процессор 1 ГГц или выше, сопоставимый с процессором Pentium, и не менее 300 МБ свободного места на диске. Она работает со следующими операционными системами:

Таблица 1. Требования системы безопасности конечных точек

Операционная система	Необходимая системная память (RAM)
Windows XP SP3	512 МБ
Windows 2003 SP2	512 МБ
Windows Vista SP1 или более новая версия	1 ГБ (32 бит), 2 ГБ (64 бит)
Windows 2008 (включая R2)	2 ГБ (64 бит)
Windows 7	1 ГБ (32 бит), 2 ГБ (64 бит)
Windows 2012 (включая R2)	2 ГБ (64 бит)
Windows 8	1 ГБ (32 бит), 2 ГБ (64 бит)
Windows 8.1	1 ГБ (32 бит), 2 ГБ (64 бит)
Windows 10	1 ГБ (32 бит), 2 ГБ (64 бит)
Windows Server 2016	2 ГБ
Mac OX 10.9+	1 ГБ
Red Hat Enterprise Linux (RHEL) 6.8, 7.2, 7.3	2 ГБ

Варианты развертывания
Система безопасности конечных точек Endpoint Security может быть развернута через облако или как виртуальное или локальное аппаратное устройство (перечислено ниже), защищающее до 100000 конечных точек. HX4502 может использоваться как для ядра, так и для развертывания DMZ — единственное различие заключается в состоянии лицензии каждого устройства; аппаратное обеспечение идентично.

Для получения дополнительной информации о FireEye, перейдите по адресу: **www.FireEye.com**

Компания Axoft является официальным дистрибутором решений FireEye в России и оказывает полный спектр услуг в части поддержки и продвижения продуктов вендора.

О компании FireEye, Inc.
FireEye - мировой разработчик решений по защите от современных киберугроз. Объединяя лучшие отраслевые технологии, многолетний опыт и аналитику, FireEye предлагаетширокий выбор универсальных адаптивных технологий для защиты от основных векторов атак, способных обходить традиционные решения на основе сигнатурного анализа, а также традиционные решения-«песочницы». Заказчики FireEye – это свыше 6 600 клиентов в 67 странах, включая более 45% из списка Forbes Global 2000.

FireEye