DATA SHEET

FireEye

Система сетевой безопасности FireEye Network Security

Эффективная защита уязвимости данных для средних и крупных организаций

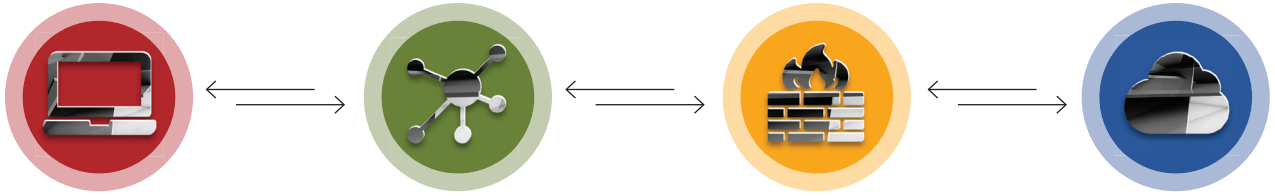
Общая информация

Система сетевой безопасности FireEye Network Security — это эффективное решение для защиты от киберугроз, помогающее организациям свести к минимуму риск дорогостоящих уязвимостей, точно обнаруживающее и немедленно останавливающее новейшие, целенаправленные и прочие трудно обнаруживаемые атаки, скрывающиеся в интернет-трафике. Она способствует эффективному разрешению обнаруженных инцидентов в системе безопасности в считанные минуты за счет интеграции конкретных доказательств, ценной оперативной информации и процесса реагирования. С системой сетевой безопасности FireEye Network Security организации эффективно защищены от современных угроз, независимо от того, используют ли они операционные системы Microsoft Windows, Apple OS X, или уязвимости приложений, направлены ли на головной офис или филиалы, скрыты ли в большом объеме входящего интернет-трафика, который должен проверяться в режиме реального времени.

В основе системы сетевой безопасности FireEye Network Security лежат технологии Multi-Vector Virtual Execution TM (MVX) (мульти-векторного виртуального исполнения) и Intelligence-Driven Analysis (IDA) (анализа оперативной информации). Мульти-векторное виртуальное исполнение MVX — это механизм динамического анализа без подписи, который проверяет подозрительный сетевой трафик для определения атак, труднообнаружимых традиционными системами защиты с подписью и на основе правил. Анализ оперативной информации IDA представляет собой набор механизмов контекстных динамических правил, которые обнаруживают и блокируют вредоносную активность в режиме реального времени и позднее, основываясь на анализе последних данных о машинах, взломщиках и жертвах. Система сетевой безопасности FireEye Network Security также включает систему предотвращения вторжений (IPS) для обнаружения распространенных атак с использованием обычного сопоставления подписей.

Система сетевой безопасности FireEye Network Security доступна в различных вариантах конструктивных параметров, развертывания и производительности. Обычно она размещается на пути интернет-трафика за традиционными устройствами сетевой безопасности, такими как межсетевой экран следующего поколения, система предотвращения вторжений IPS и защищенные интернет-шлюзы (SWG). Система сетевой безопасности FireEye Network Security дополняет эти решения, быстро обнаруживая как известные, так и неизвестные атаки с высокой точностью и низким уровнем ложноположительных срабатываний, одновременно способствуя эффективному реагированию на каждое оповещение.

Рисунок 1. Типичная конфигурация — решения для сетевой безопасности



Возможности	Преимущества
Обнаружение	
Точно обнаруживает новейшие, целенаправленные и прочие труднообнаружимые кибератаки	Минимизирует риск дорогостоящей уязвимости данных
Расширяемая модульная архитектура безопасности	Обеспечение защиты инвестиций
Постоянный уровень защиты для среды с несколькими ОС и всех точек доступа в Интернет	Создает надежную защиту всей организации для всех типов устройств
Интегрированные, распределенные, физические, виртуальные, локальные и облачные варианты развертывания	Предлагает гибкость для соответствия предпочтениям и ресурсам организации
Многовекторная корреляция с электронной почтой и безопасностью контента	Обеспечивает видимость более широкой поверхности атаки
Предотвращение	
Немедленная блокировка атак с линейной скоростью от 10 Мбит/с до 8 Гбит/с	Предоставляет защиту в режиме реального времени от труднообнаружимых атак
Реагирование	
Низкий уровень ложных оповещений, классификация потенциально опасных программ и автоматическая проверка оповещений системы предотвращения вторжений IPS	Снижает эксплуатационные расходы по сортировке ненадежных оповещений
Переориентация на оперативные данные и проверку предупреждений, ограничение конечных точек и реагирование на инциденты	Автоматизирует и упрощает рабочие процессы безопасности
Доказательства исполнения и актуальные оперативные данные об угрозах с контекстуальным аналитическим заключением	Ускоряет установление приоритета и разрешение обнаруженных инцидентов безопасности
Расширяемость от одного до тысячи сайтов	Поддерживает развитие бизнеса

Технические преимущества

Точное обнаружение угроз

Система сетевой безопасности FireEye Network Security использует множество методов анализа для обнаружения атак с высокой точностью и низким уровнем ложных оповещений:

- **Механизм мульти-векторного виртуального исполнения Multi-Vector Virtual ExecutionTM (MVX)** обнаруживает инструменты эксплуатации недокументированной уязвимости, многоконтурные и прочие труднообнаружимые атаки с помощью динамического анализа без подписи в безопасной виртуальной среде. Он предупреждает фазу заражения и компрометации в цепи остановки кибератаки путем выявления ранее не встречавшихся инструментов эксплуатации и вредоносных программ.
- **Механизмы анализа оперативной информации (IDA)** обнаруживают и блокируют вводящие в заблуждение, целенаправленные и прочие настраиваемые атаки с использованием основанного на правилах, контекстуального анализа обработки данных в реальном времени, собранных непосредственно из миллионов вердиктов мульти-векторного виртуального исполнения MVX за тысячи часов опыта реагирования на инциденты компанией Mandiant, принадлежащей FireEye, и сотнями исследователей угроз iSight. Он останавливает фазы заражения, компрометации и вторжения цепи остановки кибератаки путем выявления вредоносных инструментов эксплуатации уязвимостей, вредоносных программ и командных функций обратного вызова (CnC). Он также извлекает и отправляет подозрительный сетевой трафик для анализа и окончательного вердикта механизмом мульти-векторного виртуального исполнения MVX.
- **Структурированная оперативная информация об угрозах eXpression (STIX)** обеспечивает поглощение оперативной информации об угрозах третьих сторон с использованием стандартного отраслевого формата, добавляя персонализированные индикаторы угрозы в механизмы анализа оперативной информации IDA.

Мгновенная и безотказная защита

Система сетевой безопасности FireEye Network Security предлагает гибкие режимы конфигурирования, включая:

- Внеполосный мониторинг через TAP/SPAN, встроенный мониторинг или встроенное активное блокирование. Режим встроенной блокировки автоматически блокирует входящие инструменты эксплуатации уязвимостей, вредоносные программы и исходящие многопротокольные обратные вызовы. В режиме встроенного мониторинга генерируются оповещения, и организации решают, как им реагировать на них. В режиме внеполосного предотвращения система сетевой безопасности FireEye Network Security выдает сигнал сброса TCP для внеполосной блокировки соединений TCP, UDP или HTTP.
- Интеграция с переключателем FireEye Active Fail Open (AFO) (активного открытия при отказе) для обеспечения бесперебойной работы сети.
- Выбранные модели предлагают вариант возможности активной высокой доступности (HA) для обеспечения устойчивости в случае отказа сети или устройства.

Широкое покрытие поверхности атаки

Система сетевой безопасности FireEye Network Security обеспечивает постоянный уровень защиты сегодняшних разнообразных сетевых сред:

- Поддержка наиболее распространенных операционных систем Microsoft Windows и Apple Mac OS X
- Анализ более 140 различных типов файлов, включая портируемые исполняемые файлы (PE), веб-контент, архивы, изображения, приложения Java, Microsoft и Adobe и мультимедиа
- Проверка подозрительного сетевого трафика в отношении тысяч операционных систем, пакетов обновлений, типов приложений и комбинаций версий приложений

Проверенные и приоритетные оповещения

Помимо обнаружения истинных атак, технология мульти-векторного виртуального исполнения FireEye MVX также используется для определения надежности оповещений, обнаруженных обычными методами сопоставления подписей, и выявления и установления приоритетов критических угроз:

- Система предотвращения вторжений (IPS) с ресурсами проверки механизма мульти-векторного виртуального исполнения MVX уменьшает время, необходимое для сортировки определения на основе подписей, традиционно подверженного ложным оповещениям.
- Категоризация потенциально опасных программ отделяет истинные попытки вторжения от нежелательной, но менее вредоносной деятельности (как, например, рекламное и шпионское ПО) для установления приоритета реагирования на оповещения

Актуальный аналитический обзор угроз

Оповещения, созданные системой сетевой безопасности FireEye Network Security, включают

конкретные доказательства и контекстуальную оперативную информацию для быстрого реагирования, установления приоритета и содержания угрозы:

- **Динамическая оперативная информация об угрозах Dynamic Threat Intelligence (DTI):** конкретные данные в режиме реального времени, глобально распространяемые для быстрой и упреждающей остановки целевых и новых атак
- **Оперативная информация о новейших угрозах Advanced Threat Intelligence (ATI):** контекстный аналитический обзор атак для ускорения реагирования и предписаннного руководства для сдерживания угроз

Интеграция рабочего процесса реагирования

Система сетевой безопасности FireEye Network Security может быть дополнена несколькими способами для автоматизации рабочих процессов реагирования на оповещения:

- центральное управление FireEye Central Management соотносит оповещения от системы сетевой безопасности FireEye Network Security и системы безопасности электронной почты FireEye Email Security для более широкого обзора атаки и установления правил блокировки, предотвращающих дальнейшее распространение атаки
- система сетевой экспертизы FireEye Network Forensics интегрируется с системой сетевой безопасности FireEye Network Security для обеспечения детального захвата пакетов, связанных с оповещением, и обеспечения глубокого исследования
- система безопасности конечных точек FireEye Endpoint Security идентифицирует, проверяет и содержит риски, обнаруженные системой сетевой безопасности FireEye Network Security, для упрощения сдерживания и восстановления затронутых конечных точек

Гибкие варианты развертывания

Система сетевой безопасности FireEye Network Security предлагает различные варианты развертывания, соответствующие потребностям и бюджету организации:

- **Интегрированная система сетевой безопасности:** автономное, многофункциональное аппаратное устройство со встроенным сервисом мульти-векторного виртуального исполнения MVX для обеспечения точки доступа в Интернет на одном сайте. Система сетевой безопасности FireEye Network Security — это легко управляемая бесклиентная платформа, развертываемая менее чем за 60 минут. Она не требует регулировки, политик или настройки.
- **Распределенная сетевая безопасность:** расширяемый программно-аппаратный комплекс с централизованным общим сервисом мульти-векторного виртуального исполнения MVX для защиты точек доступа в Интернет в организациях
  - **умный узел сети Network Smart Node:** физические или виртуальные устройства, анализирующие интернет-трафик для обнаружения и блокировки вредоносного трафика и представления подозрительной активности по зашифрованному соединению с сервисом мульти-векторного виртуального исполнения MVX в целях анализа окончательного вердикта
  - **умная энергосистема мульти-векторного виртуального исполнения MVX Smart Grid:** локальный центральный адаптивный сервис мульти-векторного виртуального исполнения MVX, обеспечивающий прозрачную расширяемость, встроенную отказоустойчивость N + 1 и автоматизированную балансировку нагрузки
  - **облачное мульти-векторное виртуальное исполнение FireEye Cloud MVX:** подписка на размещенный в системе FireEye сервис мульти-векторного виртуального исполнения MVX, обеспечивающая конфиденциальность путем анализа трафика на умном узле сети Network Smart Node. Только подозрительные объекты отправляются по зашифрованному соединению на сервис мульти-векторного виртуального исполнения MVX, где отбраковываются объекты, признанные безобидными.

Рисунок 2. Примеры интегрированной сетевой безопасности включают NX 2550, NX 3500, NX 5500, NX 10450.

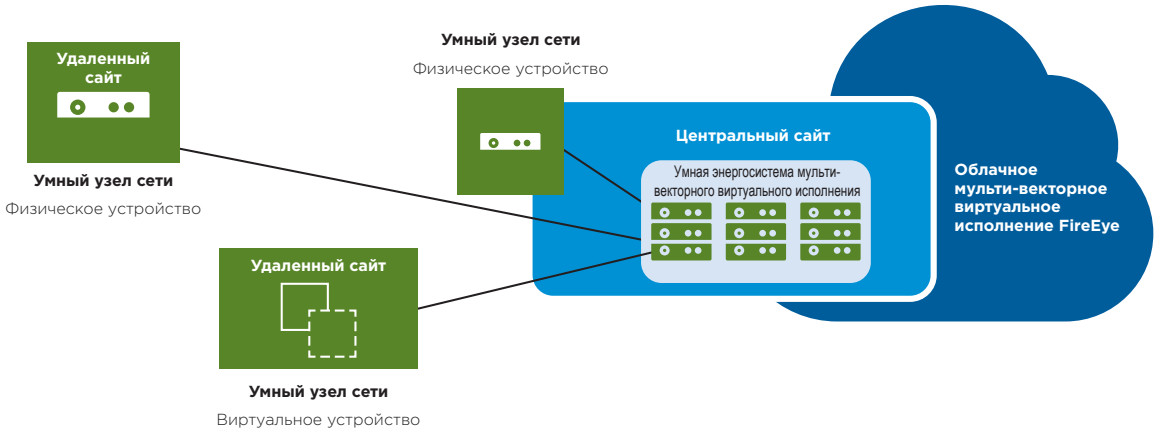


Рисунок 3. Модели распределенного развертывания для сетевой безопасности.

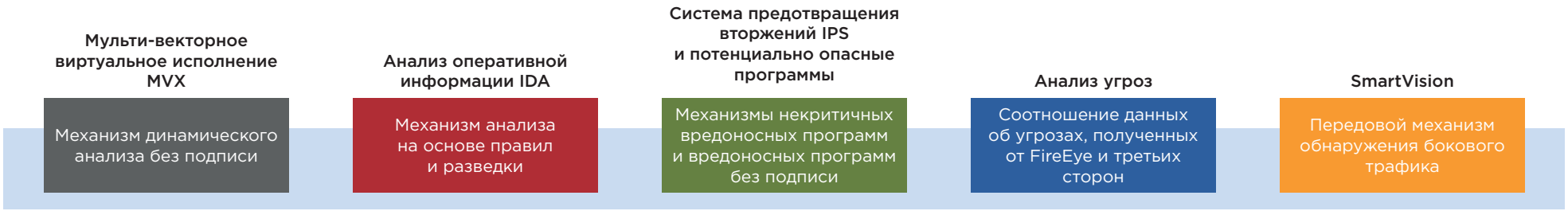


Рисунок 4. Модульные компоненты системы сетевой безопасности FireEye Network Security.

Расширяемая архитектура

Умные узлы сети FireEye Network Smart Nodes имеют модульную и расширяемую архитектуру программного обеспечения и системный дизайн для обеспечения множества возможностей защиты от угроз в качестве программных модулей.

Высокая производительность и расширяемость

Система сетевой безопасности FireEye Network Security защищает точки доступа в Интернет на линейной скорости с вариантами производительности для центральных офисов и филиалов самых разных размеров:

Расширяемая архитектура умной энергосистемы мульти-векторного виртуального исполнения MVX Smart Grid и облачного мульти-векторного виртуального исполнения FireEye Cloud MVX позволяет сервису мульти-векторного виртуального исполнения MVX поддерживать от одного до тысячи умных узлов сети Network Smart Node и расширяться по мере необходимости.

Конструктивные параметры	Производительность
Интегрированная сетевая безопасность	от 50 Мбт/с до 4 Гбт/с
Физический умный узел сети	от 50 Мбт/с до 10 Гбт/с
Виртуальный умный узел сети	от 50 Мбт/с до 1 Гбт/с

Преимущества для бизнеса

Разработанная для удовлетворения потребностей организаций с одним сайтом и множеством распределенных сайтов, система сетевой безопасности FireEye Network Security имеет несколько преимуществ:

Минимизирует риск уязвимости данных

Система сетевой безопасности FireEye Network Security — это высокоэффективное решение для кибербезопасности, которое:

- Предотвращает вторжение злоумышленников в организацию в целях кражи ценных активов или подрыва производства путем остановки продвинутых, целенаправленных и прочих труднообнаружимых атак.
- Останавливает атаки и быстрее подавляет вторжения с помощью конкретных доказательств, актуальных оперативных данных, встроенной блокировки и автоматизации рабочего процесса реагирования
- Исключает слабые места киберзащиты организации с последовательной защитой различных операционных систем, типов приложений, сайтов филиалов и центральных офисов

Быстрая окупаемость

Согласно недавнему исследованию Forrester Consulting (Forrester (май 2016 г.) Совокупный экономический эффект FireEye), клиенты системы сетевой безопасности FireEye Network Security могут рассчитывать на экономию средств на 152% за три года, а первоначальные инвестиции окупятся всего за 9,7 месяцев. Система сетевой безопасности FireEye Network Security:

- Фокусирует ресурсы отдела безопасности на реальных атаках для снижения операционных расходов.
- Оптимизирует финансовые затраты с помощью общего сервиса мульти-векторного виртуального исполнения MVX и большого количества точек производительности для правильного определения масштаба развертывания в соответствии с требованиями.
- Поддерживает в актуальном состоянии инвестиции в безопасность за счет плавной расширяемости при увеличении числа филиалов или объема интернет-трафика.
- Защищает существующие инвестиции, позволяя без затрат переходить от интегрированного к распределенному развертыванию.
- Сокращает будущие капиталовложения за счет модульной и расширяемой архитектуры.

Награды и сертификаты

Портфель решений системы сетевой безопасности FireEye Network Security был награжден рядом отраслевых и правительственных наград и сертификатов:

- В 2016 году Frost & Sullivan признала FireEye бесспорным лидером на рынке с долей рынка 56% — больше, чем у 10 следующих конкурентов вместе взятых (Frost & Sullivan (октябрь 2016 г.). Анализ рынка сетевой безопасности Sandbox).
- Система сетевой безопасности FireEye Network Security получила множество наград от института SANS, журнала SC Magazine, CRN и других организаций
- Система сетевой безопасности FireEye Network Security стала первым решением по безопасности на рынке, получившим сертификацию Министерства национальной безопасности США.