



## Форсируйте защиту

Повышайте уровень защиты и реагирования на события безопасности благодаря автоматизированному сбору информации о событиях в сети

Атаки редко бывают разрозненными, а вот защитные программы часто действуют поодиночке. Разобщенные между собой технологии безопасности и неэффективные системы реагирования на события оставляют организации чрезвычайно уязвимыми перед лицом изощренных угроз. Для создания успешно работающей системы безопасности организациям необходимо объединить точную интегрированную защиту сетей с программой консолидированного автоматизированного мониторинга. Платформа McAfee® Network Security Platform и решение McAfee® Enterprise Security Manager объединяют защиту сетей в режиме реального времени, ситуационную осведомленность на всех уровнях предприятия и быстро реагирующую платформу для анализа событий безопасности в единое «бесшовное» интегрированное решение, которое способно выявить и заблокировать больше угроз и одновременно обеспечить быстрое реагирование на успешно начинающиеся атаки.

### Форсированная защита. Быстрая, точная, эффективная

Скорость имеет значение. Организации полагаются на то, что их системы сетевой защиты соответствуют требованиям сети и могут обнаруживать угрозы в режиме реального времени. И если речь идет о реагировании на инцидент безопасности, то счет идет на секунды.

Решение McAfee объединяет в себе ведущие технологии систем предотвращения вторжений (IPS) и систем управления информацией о безопасности и событиях безопасности (SIEM), предлагая программу защиты на основе оценки рисков и высокого уровня ситуационной осведомленности. Кроме того, решение обеспечивает высочайшую производительность, позволяя принимать меры в режиме реального времени. McAfee® Network Security Platform сочетает в себе средства однопроходной проверки трафика на основе протоколов со специальным аппаратным обеспечением операторского класса, что позволяет в реальных условиях осуществлять проверку трафика со скоростью свыше 10 Гбит в секунду на одном единственном устройстве. Чрезвычайная эффективность ее архитектуры позволяет сохранять высокий уровень быстродействия независимо от настроек безопасности, в то время как у других систем IPS при использовании политик, ставящих безопасность выше быстродействия, сокращение пропускной способности может составить до 50 процентов.

McAfee Enterprise Security Manager объединяет насыщенный поток событий, направляемый с платформы McAfee Network Security Platform и содержащий всю информацию о событиях безопасности предприятия, и автоматически связывает насыщенную контекстную информацию об активах, пользователях, угрозах и данных в нашей проприетарной базе данных, созданной для обработки больших объемов данных в сфере безопасности. Насыщенный контекст в сочетании с самой быстрой из имеющихся на рынке платформой управления данными о безопасности дает картину внутренних и внешних рисков в режиме реального времени, а при возникновении инцидентов обеспечивает поддержку запросов на принятие ответных мер в течение секунд, а не минут или часов.

### Превратите свою ИТ-инфраструктуру в объединенную систему защиты с помощью технологии McAfee Global Threat Intelligence!

Хотели бы вы превратить переключатели, маршрутизаторы, серверы и другие элементы ИТ-инфраструктуры в мощные инструменты защиты? Именно это и делает наша технология McAfee Global Threat Intelligence™ (McAfee GTI™), которая теперь включена в решение McAfee Enterprise Security Manager. Решение кардинально повышает эффективность защиты благодаря прогнозной информации об угрозах, собираемой в режиме реального времени по всему миру. В McAfee Network Security Platform используется технология McAfee GTI, динамически влияющая на процесс предотвращения известных и новых атак в реальном масштабе времени. Технология McAfee GTI проводит оценку репутации передаваемой по сети информации на основе получаемых со всего света данных о репутации миллиардов отдельных файлов, IP-адресов, URL-адресов, протоколов и географических точек.

Этот массивный поток данных используется решением McAfee Enterprise Security Manager для автоматического обнаружения связи с известными злоумышленниками путем сопоставления IP-адресов злоумышленников с IP-адресами, выявленными любым устройством McAfee или устройством другой компании. Кроме того, McAfee Enterprise Security Manager хранит архив годами собираемых данных компьютерно-технической экспертизы, что позволяет быстро найти весь трафик, ассоциированный с вновь обнаруженным злоумышленником.

#### **Бесшовная платформа для реагирования на инциденты**

Платформа McAfee Network Security Platform быстро блокирует вредоносный трафик за счет передовых функций обнаружения угроз. Функция анализа тенденций решения McAfee Enterprise Security Manager позволяет без труда обнаружить повторные попытки атак с помощью автоматической быстро реагирующей платформы для анализа событий безопасности. Решение McAfee Enterprise Security Manager дает аналитикам в сфере безопасности более широкое представление о злоумышленниках. Теперь вместо «моментального снимка» злоумышленника аналитик получает архив событий прошлых дней, месяцев и даже лет. Быстро реагирующая база данных McAfee Enterprise Security Manager в сочетании с интуитивно понятным пользовательским интерфейсом превращает ответы на неотложные вопросы, касающиеся реагирования на инциденты, в прямые рекомендации для аналитиков по безопасности.

