# McAfee Application Data Monitor

## Обнаружение скрытых угроз путем проверки трафика на уровне приложений

Устройство McAfee® Application Data Monitor обеспечивает защиту и нормативно-правовое соответствие не только за счет управления журналами, но также благодаря мониторингу вплоть до уровня приложения. Оно позволит вам выполнять полную проверку содержимого приложений и осуществлять сбор подробнейшей информации за использованием вашей сети.

Устройство McAfee Application Data Monitor выполняет дешифрование полного сеанса приложения до уровня 7, обеспечивая комплексный анализ всей информации — от используемых протоколов и целостности сеанса до содержимого приложения, такого как текст электронного письма или вложений к нему. Такой уровень детализации позволяет выполнять точный анализ реального использования приложения, одновременно обеспечивая принудительное применение политик использования приложения и обнаружение скрытого вредоносного трафика.

Благодаря такой глубокой проверке обеспечивается нормативно-правовое соответствие за счет отслеживания всех случаев использования конфиденциальных данных в вашей сети. Когда устройство McAfee Application Data Monitor обнаруживает нарушение политики, оно сохраняет всю информацию о данном сеансе приложения для последующего реагирования на инциденты, компьютерно-технической экспертизы и аудита нормативно-правового соответствия.

Помимо указанных возможностей, устройство McAfee Application Data Monitor обеспечивает сбор информации об угрозах, которые могут маскироваться под разрешенные приложения, включая следующие:

- сложные угрозы безопасности уровня приложения;
- несанкционированное использование и кража конфиденциальных данных;
- атаки на «мертвые зоны» системы безопасности и атаки изнутри таких зон;
- использование опасного унаследованного кода;
- кража или неправомерное использование учетных данных пользователей;
- передача конфиденциальных данных через любое приложение;
- нарушенные бизнес-процессы.

### Ключевые преимущества

- Выполняет дешифрование полного сеанса приложения до уровня 7 для сотен приложений.
- Включает встроенные правила обнаружения конфиденциальной информации и данных, регулируемых правовыми актами.
- Поддерживает задаваемые пользователями словари и правила для выполнения индивидуальной настройки.
- Генерирует полный журнал аудита событий приложения для обеспечения нормативно-правового соответствия.
- Работает в пассивном режиме во избежание конфликта приложений.
- Интегрируется с решением McAfee Enterprise Security Manager, позволяя сопоставлять содержимое приложений с событиями и другими потоками данных.
- Наличие смешанных вариантов поставки с использованием физических и виртуальных устройств.

## Утечка данных и нарушения нормативно-правового соответствия

Устройство McAfee Application Data Monitor обнаруживает передачу конфиденциальной информации во вложениях к электронным письмам, в мгновенных сообщениях, при передаче файлов, в сообщениях, отправляемых по протоколу HTTP, или в любом другом приложении. При этом оно отправит вам немедленное уведомление, позволяя тем самым снизить ущерб от утечки данных.

Для обнаружения конфиденциальной информации, в том числе данных кредитных карт и паспортных данных, вы можете использовать готовые настройки или же выполнить индивидуальную настройку параметров устройства McAfee Application Data Monitor, создав собственные словари конфиденциальной и секретной информации. Устройство McAfee Application Data Monitor установит тип этих конфиденциальных данных, оповестит соответствующих специалистов и зарегистрирует нарушение в журнале аудита.

## Обнаружение документов

Устройство McAfee Application Data Monitor обнаруживает более 500 типов документов во время их передачи в сети с помощью электронной почты, чата, одноранговой связи, обмена файлами и других способов связи. Кроме того, оно обнаруживает документы независимо от их расширения, в том числе документы, маскирующиеся под документы других типов в попытке обойти шлюзы электронной почты и устройства систем обнаружения и предотвращения вторжений (IDS/IPS — Intrusion Detection System/Intrusion Prevention System). Устройство обнаруживает даже документы, встроенные внутрь других документов, а также архивированные, сжатые и зашифрованные документы; одновременно предоставляя параметры, необходимые для принятия мер, например имя файла и тип выполняемой операции.

## Угрозы на уровне приложений

Для проникновения в вашу сеть и вывода конфиденциальных данных новые изощренные угрозы используют уязвимости, присущие распространенным бизнес-приложениям. В то время как обнаружение подобных угроз уровня приложения с помощью традиционных брандмауэров и систем обнаружения и предотвращения вторжений является затруднительным, устройство McAfee Application Data Monitor способно исследовать все содержимое приложения (включая используемые протоколы) для обнаружения скрытых вредоносных нагрузок, вредоносных программ и даже скрытых каналов связи, например исполняемых файлов (*.exe), встроенных в PDF-документы.

## Аномалии протоколов

Выявление аномалий обеспечивает упреждающее обнаружение надвигающихся угроз, снижение уровня риска и сокращение до минимума утечки данных. Если традиционные решения защиты ограничиваются анализом сетевых потоков, то устройство McAfee Application Data Monitor работает на более высоком уровне. Мы анализируем предысторию поведения в сети с целью выявления аномалий в приложениях и протоколах, предлагая более надежные упреждающие методы обнаружения риска.

## Более 500 поддерживаемых приложений и протоколов

- **Сетевые протоколы нижнего уровня:** TCP/IP, UDP, RTP, RPC, SOCKS, DNS и другие
- **Электронная почта:** MAPI, NNTP, POP3, SMTP, Microsoft Exchange
- **Веб-почта:** AOL Webmail, Hotmail, Yahoo! Mail, Gmail, Facebook и электронная почта MySpace
- **Обмен мгновенными сообщениями:** AOL, ICQ, Jabber, MSN, SIP и Yahoo!
- **Протоколы передачи файлов:** FTP, HTTP, SMB и SSL
- **Протоколы сжатия и извлечения файлов:** BASE64, GZIP, MIME, TAR, ZIP и другие
- **Архивирование файлов:** форматы RAR, ZIP, BZIP, GZIP, Bin-hex и кодирование Unix-Unix
- **Установочные пакеты:** пакеты Linux, CAB-файлы InstallShield, CAB-файлы Microsoft
- **Файлы изображений:** GIF, JPEG, PNG, TIFF, AutoCAD, Photoshop, Bitmap, Visio, Digital RAW и иконки Windows
- **Аудиофайлы:** WAV, MIDI, RealAudio, Dolby Digital AC-3, MP3, MP4, MOD, RealAudio, SHOUTCast и другие
- **Видеофайлы:** AVI, Flash, QuickTime, Real Media, MPEG-4, Vivo, Digital Video (DV), Motion JPEG и другие

## Никакого вмешательства в работу приложений

Поскольку устройство McAfee Application Data Monitor использует для работы порт SPAN, то оно не влияет на быстродействие и надежность приложения и не вызывает задержек.

## Интеграция в вашу инфраструктуру

В отличие от большинство решений для мониторинга сети, которые действуют изолированно друг от друга, устройство McAfee Application Data Monitor работает согласовано с другими системами информационной безопасности. Подключаясь к вашей инфраструктуре безопасности через McAfee Enterprise Security Manager, устройство упрощает операции по обеспечению безопасности, повышает общий уровень эффективности и снижает расходы. Вы можете объединить продукты, предназначенные для обнаружения мошенничества и утечки данных, с мощными функциями анализа, инструментами проверки сети, мониторинга событий баз данных и проч.

## Примеры использования

Устройство McAfee Application Data Monitor может обнаруживать целый ряд несанкционированных действий, включая нарушение политик, кражи и мошенничество. Вот несколько примеров:

### Кража конфиденциальной информации

Сотрудник компании, вошедший в систему под именем i.petrov@company.ru, отправил электронное сообщение по адресу koresh@yandex.ru. Электронное сообщение содержало во вложении файл shoo.doc, в котором встречались слова «секретная формула». Электронное сообщение было отправлено в 12:20 локального рабочего стола 0232 (192.168.0.36) через сервер SMTP (10.0.2.13); в качестве темы сообщения была указана фраза: «он у меня».

### Использование несанкционированных приложений

Сотрудник компании нарушил политику, передав музыкальный файл с помощью приложения для обмена файлами между пользователями, которое он сам и установил. Он передавал файлы большого объема в рабочее время, потребляя ценную полосу пропускания. Более тщательное расследование показало, что этот сотрудник регулярно нарушает политику безопасности, используя протоколы Jabber и IRC и установив на своем компьютере несанкционированный веб-сервер.

## Более 500 поддерживаемых приложений и протоколов (продолжение)

- **Другие приложения и файлы:** базы данных, таблицы, факсы, веб-приложения, шрифты, исполняемые файлы, приложения Microsoft Office, игры и даже инструменты для разработки программного обеспечения
- **Другие протоколы:** сетевой принтер, доступ к оболочке, VoIP и одноранговая связь

### Использования Интернета в личных целях в рабочее время

Сотрудница компании тайно занимается внутридневной торговлей, для чего в рабочее время подключается к финансовым и трейдинговым сайтам. В среднем продолжительность подключения составляет один час в первой половине дня и один час во второй. Кроме того, она пользуется корпоративной системой VoIP (SIP) для совершения в среднем шести звонков в день и часами использует сервис Yahoo! Messenger, зарегистрировавшись как broker_sanya и обмениваясь сообщениями с broker_kolyan и broker_milashka.

### Использование слабых паролей

В соответствии с политикой безопасности вашей компании для всех пользовательских систем и учетных записей приложений требуется использование надежных паролей. Учетные записи Microsoft Active Directory подлежат строгому контролю. Однако десятки слабых паролей по-прежнему используются на внешних FTP-серверах, почтовых серверах и критически важных веб-приложениях, которые не применяют службу Active Directory.

## Дополнительная информация

Для получения более подробных сведений посетите наш сайт **www.mcafee.com/ru/products/siem/index.aspx**.

McAfee Ireland Ltd.
Building 2000, City Gate
Mahon, Cork, Ireland
www.mcafee.com/ru


61322ds_app-data-monitor_0914
Сентябрь 2014 г.