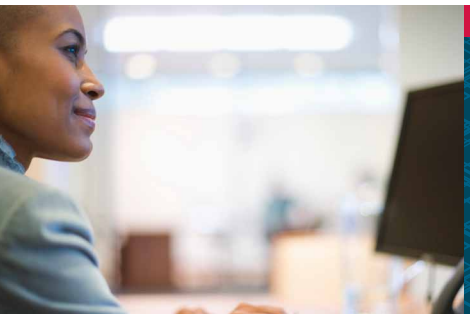

# Эволюционирующий характер средств защиты настольных компьютеров

Эволюция средств защиты настольных компьютеров проходила под воздействием целого ряда разных факторов, включая наличие вредоносных программ, направленных на конкретные цели; соображения удобства для конечных пользователей; а также расходы на ИТ-поддержку и ИТ-операции. Внедрение традиционных средств защиты настольных компьютеров напоминает приобретение страхового полиса для защиты от возможных рисков, в котором, однако, не учтены в достаточной мере никакие другие факторы. В корпоративных условиях общего операционного окружения обеспечение безопасности настольных компьютеров поставило перед ИТ-отделами задачу нахождения компромисса между обеспечением свободы действий конечных пользователей и требованиями безопасности.

## Настольные среды

Как показывают результаты целого ряда исследований, существует две разновидности настольных сред:

- *для стандартных пользователей* — Образы «общего операционного окружения» с ограниченным (фиксированным) набором функций и настольные системы, устанавливаемые с общего образа. В таких средах конечный пользователь не имеет прав для установки и удаления программного обеспечения. *Примерами образов «общего операционного окружения»* являются рабочие станции в предприятиях розничной торговли, финансовых учреждениях и больницах.
- *для опытных пользователей:*пользователи имеют возможность устанавливать свое собственное программное обеспечение. *Примерами сред для опытных пользователей являются* инженерные среды и среды для создания графического дизайна.

В настоящем документе мы остановимся на модели обеспечения безопасности «общего операционного окружения».

## Актуальные проблемы безопасности настольных сред

За последние 20 лет, с тех пор как наше общество стало развиваться в сторону «экономики знаний», задача обеспечения безопасности и надежности ИТ-инфраструктуры стала намного более актуальной. Произошел значительный рост количества вредоносных программ, обнаруживаемых специалистами по безопасности по всему миру: с 1 000 образцов в год до 1 000 образцов в день. Что касается операционного уровня, то средства защиты конечных точек (настольных компьютеров и ноутбуков) стали более сложными, а руководители отделов ИТ-безопасности нередко говорят о том, что стоящие перед ними задачи обусловлены не только борьбой с угрозами, но и решением вопросов операционной безопасности.

### Взрывной рост количества вредоносных программ

Наибольшую озабоченность у руководителей отделов безопасности вызывает феноменальный рост количества находящихся в обращении вредоносных программ. Наблюдается заметный рост степени сложности и количества вредоносных программ, что ведет к появлению большого числа векторов для атак на ИТ-инфраструктуру.

### Быстродействие

Во-вторых, озабоченность по-прежнему вызывает уровень быстродействия традиционных решений, и причиной тому отчасти является значительное увеличение числа используемых сигнатур.

### Операционная безопасность

В-третьих, большую озабоченность вызывает операционный аспект обеспечения безопасности. Проходя через ИТ-окружение, вредоносная программа ослабляет инфраструктуру безопасности. Кроме того, традиционные решения для обеспечения безопасности на основе сигнатур не всегда в состоянии противостоять атакам нулевого дня и постоянным угрозам повышенной сложности (advanced persistent threats — APTs).

### Распространение неавторизованных приложений

И, наконец, особую озабоченность вызывает распространение неавторизованных приложений на настольных компьютерах конечных пользователей. На развивающихся рынках данная проблема существует бок о бок с проблемой распространения в корпоративной среде пиратского и нелицензионного программного обеспечения.

### Поведенческие аспекты управления средствами защиты

Что касается поведенческих аспектов, то в «общих операционных окружениях» наблюдается постоянная борьба между обязанностью администратора обеспечить безопасность и стремлением конечного пользователя работать в безопасной среде, дающей полную свободу действий. Потребности обеих сторон должны быть учтены без ущерба для безопасности и производительности труда внутри организации. Необходимо найти такое решение, которое будет соответствовать требованиям к безопасности, выдвигаемым как администратором, так и пользователем, и не будет при этом нарушать принцип приоритета стабильной производительности труда.

## Куда обратиться за помощью?

Благодаря методу белых списков McAfee® Application Control, если его использовать в сочетании с традиционной антивирусной технологией, будет надежным решением для многих из этих проблем. McAfee Application Control работает заметно лучше, чем традиционные средства защиты настольных компьютеров, позволяя не только бороться с вредоносными программами, но и повысить потенциал противостояния распространению вирусных эпидемий.

### Белые списки приложений

В основе метода белых списков лежит определение файлов с «известной хорошей» репутацией для данной ИТ-среды, и допуск в систему только таких файлов. Реализация этого метода допускает множество вариантов: с одной стороны, такие системы могут развертываться автономно; с другой стороны, метод белых списков можно использовать наряду с традиционным решением на основе черных списков, таким как антивирусная программа. Здесь мы поговорим об ИТ-среде с антивирусным решением, эффективность которого может быть повышена путем реализации метода белых списков.

### Режим наблюдения

McAfee Application Control может работать в так называемом «режиме наблюдения». В этом режиме McAfee Application Control не осуществляет применение политик, а только мониторинг. «Режим наблюдения» можно активировать после установки McAfee Application Control и получения списка имеющихся приложений (путем сканирования систем). Если организация проводит развертывание средств защиты впервые, то этот режим можно использовать для составления политик, позволяющих обнаруживать случаи несоответствия стандартам безопасности, и для определения допустимых операционных исключений из правил.

Если развернуть «режим наблюдения» вместе с традиционным антивирусным решением, то антивирусное решение можно продолжать использовать в качестве основного средства защиты. Благодаря этому администратор средств защиты может продолжать мониторинг ИТ-активов, а задачу обеспечения собственно безопасности на пользовательских конечных точках выполняет антивирусная программа. В результате уровень производительности пользователей настольных систем растет, а ИТ-администраторы получают возможность получить более полную картину о состоянии системы безопасности организации.

### Анализ репутации файлов с помощью McAfee Global Threat Intelligence™ (McAfee GTI™)

McAfee Application Control включает в себя также функции анализа репутации файлов на основе технологии McAfee GTI. Получив от McAfee Application Control полный список файлов на конечных точках, McAfee® ePolicy Orchestrator® (McAfee ePO™) сопоставляет его с показателями репутации файлов, полученными с сервера McAfee GTI. Это дает возможность в автономном режиме и без дополнительной нагрузки на систему выявлять вредоносные и иного рода сомнительные файлы в корпоративной среде. Если файл указан как вредоносный, то интерфейс McAfee ePO дает возможность быстро обнаружить место нахождения всех экземпляров данной вредоносной программы в масштабах всей ИТ-среды.

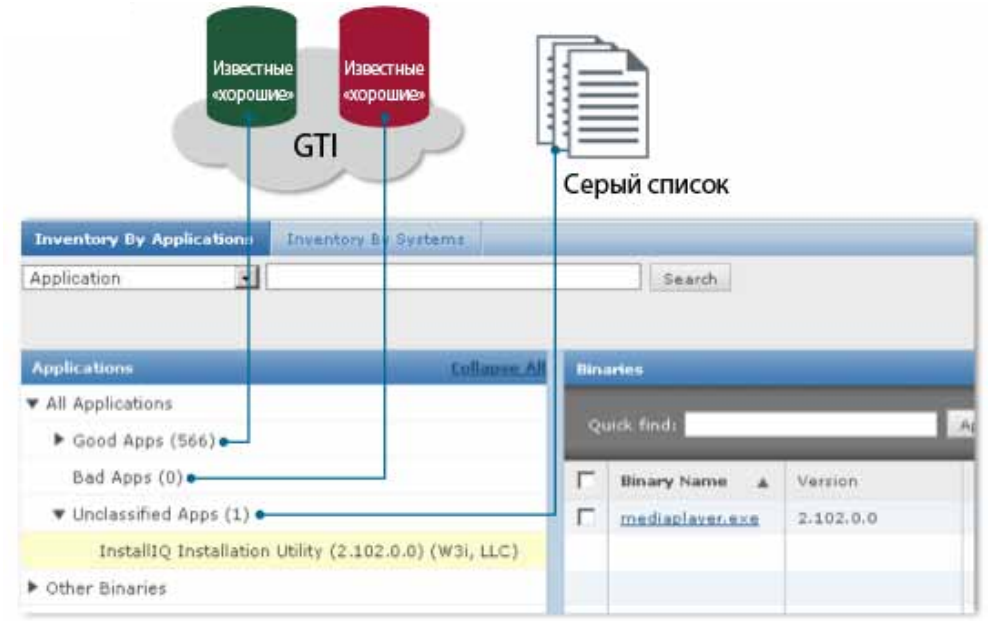


Рис. 1. Каждое используемое в компании приложение классифицируется на основе анализируемой McAfee GTI репутации файлов.

### Борьба с эпидемиями вредоносных программ

Использование McAfee Application Control в «режиме наблюдения» в сочетании с антивирусной программой, являющейся основным средством защиты, дает вам уникальное преимущество в деле борьбы с эпидемиями вредоносных программ. Кроме того, в зависимости от обстоятельств, администратор может переходить из «режима наблюдения» в «режим применения политик» и обратно. Если при первых же признаках эпидемии вредоносных программ перевести McAfee Application Control в «режим применения политик», то состояние систем будет «заморожено» в масштабах всей ИТ- инфраструктуры и вредоносные программы не смогут распространиться дальше вглубь организации. В сочетании с программным обеспечением McAfee ePO, дающим возможность управлять процессом обнаружения вредоносных программ на основе списков файлов, это позволяет упростить и ускорить процесс восстановления зараженных систем.

### Динамическое составление белых списков путем взаимодействия с пользователями

И наконец, если McAfee Application Control развернут в «режиме применения политик» и, следовательно, обеспечивает более высокий уровень защиты, то для внесения изменений в свои системы конечный пользователь должен подать соответствующий запрос в отдел ИТ. В этом и заключается динамическая составляющая метода белых списков, построенная на четко определенном взаимодействии между пользователем и администратором. Благодаря этой функции McAfee Application Control может обеспечивать более высокий уровень защиты при сохранении того же уровня комфорта для пользователя, что и в случае использования традиционных антивирусных решений.


Рис. 2. Уведомления на рабочем столе и запрос подтверждения для приложений, не внесенных в белый список.

### Контроль за неавторизованными приложениями

На развивающихся рынках контекст обеспечения безопасности определяется также наличием возможности отслеживать попадающие в ИТ-среду неавторизованные и небезопасные программы. Поскольку список файлов доступен на уровне программного обеспечения McAfee ePO, его можно экспортировать и согласовать с корпоративным списком авторизованных и безопасных программ. Обнаруженное расхождение между согласованным корпоративным списком программ и списком файлов, экспортированным с помощью программного обеспечения McAfee ePO, позволяет выявить нарушения общих политик безопасности и лицензионных требований, если таковые имеются.

## Заключение

Для определенной категории настольных систем метод белых списков приложений постепенно становится надежным средством защиты первого уровня. Если использовать этот метод в сочетании с имеющимися антивирусными решениями, то он не только обеспечивает надежную защиту от таких новых угроз, как APT и целенаправленные вредоносные программы, но и способствует сокращению операционных расходов за счет предотвращения стихийного распространения неавторизованных приложений. Указанные нами дополнительные возможности метода белых списков приложений и появившиеся недавно технологические новшества, позволяющие легче реализовывать метод белых списков, дают администраторам надежду на появление более простой модели обеспечения безопасности настольных систем.

## О компании McAfee

McAfee — стопроцентная дочерняя компания Intel Corporation (NASDAQ: INTC), является крупнейшим в мире предприятием, специализирующейся на технологиях информационной безопасности. Компания McAfee поставляет проверенные упреждающие решения и услуги, которые обеспечивают безопасность систем, сетей и мобильных устройств по всему миру, позволяя пользователям безопасно работать и совершать покупки в Интернете. Наличие непревзойденной технологии Global Threat Intelligence, позволяет компании McAfee создавать инновационные продукты, которые помогают частным пользователям, компаниям, государственным организациям и поставщикам услуг Интернета обеспечивать соответствие нормативно-правовым требованиям, защищать данные, предотвращать нарушения работы, определять уязвимости, а также постоянно следить за уровнем собственной безопасности и повышать его. Компания McAfee непрерывно ведет постоянный поиск новых путей защиты своих клиентов. www.mcafee.com/ru

McAfee
An Intel Company

ООО «МакАфи Рус»
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
Бизнес центр «Башни на набережной»
4ый этаж, офис 405 – 409
Телефон: +7 (495) 967 76 20
Факс: +7 (495) 967 76 00
www.McAfee.ru


41101brf_desktop-security_0112_fnl_ETMG