

## Защита конечных точек для корпораций и крупного бизнеса

### В этом обзоре:

- **McAfee Total Protection for Enterprise (стр. 4)**
- **Sophos Endpoint Security and Control 7.0 (стр. 6)**
- **Symantec Client Security 3.1 (стр. 9)**

В связи с ростом сложности и размера той информации, которая обрабатывается сегодня на рабочих станциях и серверах, традиционные подходы к обеспечению безопасности в корпорациях, заключенные в защите, в первую очередь, периметра корпоративной сети, уже не являются столь эффективными, как раньше. Подход «железная защита периметра и программная внутри сети» сегодня начинает устаревать. Для обеспечения актуальной защиты корпорациям все чаще требуется более глубокий уровень защиты, заключенный в обращении большего внимания к защите конечных точек.

Можно привести много причин в защиту нового подхода. Например, корпоративные сети сегодня не имеют четко обозначенного периметра. Популярность беспроводных соединений растет с каждым днем. Мобильные сотрудники выходят в сеть за пределами корпоративной защиты из дома или других мест и подвергаются риску, оставаясь незащищенными. Вследствие этого возможность заражения сети повышается, когда такие сотрудники возвращаются в офис и подключаются к информационным ресурсам компании. Увеличение использования защищенных протоколов SSL

или организация VPN-сетей становится критической необходимостью для увеличения степени защиты соединений типа точка-точка. Однако это приводит к потере прозрачности управления безопасностью периметра, так как зачастую трудно проследить и

отфильтровать ту информацию, которая проходит через защищенные зашифрованные каналы.

**«Идеальным решением для защиты конечных точек на уровне крупного бизнеса было бы решение, полностью покрывающее три направления: тип тех конечных точек, которое оно защищает, типы угроз, от которых оно защищает, и те механизмы, которое использует данное решение для организации защиты»**

В то же время, информационные угрозы эволюционируют, становятся более сложными, распространяются быстрее и используют много технических новинок, что позволяет им успешно пробивать отдельные уровни безопасности.

**«Отложенная инсталляция, это каждодневная длительная работа по управлению, сбору отчетов и анализу тревожных ситуаций, которая в итоге сможет понизить общую стоимость владения решением по безопасности»**

Продукты для защиты конечных точек могут кардинально изменить общую картину корпоративной защиты, дополняя традиционную защиту периметра (сетевые экраны, роутеры и т.д.) тем программным обеспечением, ко-

торое устанавливается на защищаемых рабочих станциях и файловых серверах. Защита конечных точек повышает общий уровень безопасности за счет того, что угрозы, каким-либо образом прошедшие через защиту периметра, все равно будут блокированы на конечных точках и обезврежены.

Базовая часть эффективной системы защиты конечных точек должна включать в себя: антивирус, подсистему защиты от программ-шпионов (spyware), поведенческий анализатор, а также брандмауэр для рабочих станций. Все это вместе должно управляться посредством задания корпоративных политик безопасности. В данном обзоре лаборатория Cascadia Labs проведет сравнительное тестирование трех, лидирующих на данный момент, продуктов для защиты конечных точек, через призму того, как они выполняют возложенные на них современные требования к обеспечению безопасности.

### **Идеальная система безопасности**

Идеальным решением для защиты конечных точек на уровне крупного бизнеса было бы решение, полностью покрывающее три направления: типы тех конечных точек, которое оно защищает, типы угроз, от которых оно защищает, и те механизмы, которое использует данное решение для организации защиты.

Под полным покрытием системы безопасности конечных точек понимается наличие программного обеспечения, которое могло бы работать и на серверах, и на мобильных и стационарных рабочих станциях, под управлением наиболее популярных операционных систем – Windows, Linux и Macintosh.

РЕЙТИНГОВАЯ ТАБЛИЦА			
Категория	McAfee Total Protection for Enterprise	Sophos Endpoint Security and Control 7.0	Symantec Client Security 3.1
Инсталляция и Разворачивание	▲▲	▲▲▲▲▲▲	▲▲▲
Удобство и Управление	▲▲	▲▲▲▲	▲▲▲
Эффективность	▲▲▲	▲▲▲▲	▲▲▲
Быстродействие	▲▲▲	▲▲▲▲	▲▲▲▲
<b>ИТОГО</b>	▲▲▲	▲▲▲▲	▲▲▲
<b>Выводы</b>	Продукт McAfee Total Protection for Enterprise предлагает гибкую систему конфигурирования и настройки, однако он слишком сложен в использовании	Sophos Endpoint Security and Control комбинирует в себе мощную систему управления безопасности, предлагая хороший уровень защиты при высоком быстродействии	Symantec Client Security 3.1 – это качественный но не выдающийся продукт, проигрывающий конкурентам по многим характеристикам
<b>Поддерживаемые платформы</b>	Windows Vista, XP, 2003, 2002, NT, NetWare	Windows Vista, XP, 2003, 2002, NT, 95/98/Me, Macintosh, Linux, NetWare, Windows Mobile	Windows XP, 2000, 2003, NetWare
<b>Техническая поддержка</b>	24/7	24/7	В рабочее время

Обозначения: ▲ – плохо, ▲▲ – удовлетворительно, ▲▲▲ – средне, ▲▲▲▲ – хорошо, ▲▲▲▲▲ – отлично

Под полной защитой от информационных угроз понимается наличие в программном обеспечении систем защиты от известных вирусов (посредством сигнатурного анализа), включая их различные варианты; от неизвестных новых вирусов и угроз нулевого дня, которые эксплуатируют различные уязвимости в операционных системах и приложениях; угроз, возникающих в результате действия программ зомбирования компьютеров и различных троянских программ; и наконец, набор механизмов для авторизации потенциально нежелательных приложений (PUA), включающих в себя программы-рекламы, и системы удаленного управления. Кроме этого, такое защитное ПО должно обладать возможностью распознавать подозрительные действия приложений, например такие как удаление ключей из реестра Windows, или модификация системных папок, а также способностью защищать от переполнения буфера.

Наличие всех этих механизмов защиты является необходимым, но не достаточным условием в случае, если мы говорим о продукте информационной защиты корпоративного класса. Как и в случае любого крупного продукта, корпоративные пользователи при его использовании сталкиваются с

целым набором проблем, касающихся инсталляции и настройки, конфигурирования, каждодневного администрирования, задания корпоративных политик и использования системы отчетов. Теоретически система безопасности может быть сколь угодно эффективна, но на практике безопасность будет настолько сильной, насколько сильна система мониторинга текущего состояния и конфигурирования.

**«Для крупного бизнеса, где ценят простоту и прозрачность управления, продукты Sophos серьезно выигрывают перед продуктами McAfee и Symantec, в особенности в том, что касается решения каждодневных проблем без нанесения ущерба ключевой функциональности»**

Если говорить более определенно, администраторы должны обладать возможностью быстро и просто определять рабочие станции, на которых не обновлен антивирус, или станции, не отвечающие корпоративным политикам безопас-

ности, которые могут быть использованы как мостик для заражения всей корпоративной сети. Администраторы также должны иметь возможность задавать сканирование по расписанию, контролировать текущий статус и создавать отчеты, показывающие реальную ситуацию с безопасностью. В идеале, все вышеназванные возможности должны иметь унифицированный доступ и представление посредством единой системы управления, которая должна органично вливаться в общую систему ИТ-управления и иметь интеграцию с такими механизмами как Active Directory.

**Тестируемые продукты**

Для составления данного обзора были выбраны три продукта от компаний, заявленных как лидеров рынка информационной безопасности, набор функциональности которых мог бы удовлетворить всем строгим требованиям в области защиты крупного бизнеса. Все три продукта от McAfee, Sophos и Symantec представляют собой комплексные системы безопасности с защитой от вирусов, программ-шпионов и угроз «нулевого дня». В рамках данного обзора мы не рассматривали продукты или их компоненты, связанные с фильтрацией почтового трафика от вирусов и спама.

Каждый из рассматриваемых продуктов поставляется в «коробочном» виде, с лицензией на 12 или более месяцев. McAfee и Sophos в рамках лицензии предлагают также техническую поддержку в режиме 24/7, Symantec предлагает круглосуточную поддержку только как дополнительную платную опцию.

**Полученные данные**

Все три продукта тестировались в первую очередь с той точки зрения, что каждый из них должен как можно более полно решать задачи безопасности на уровне крупного бизнеса. Другими словами, ни один из протестированных продуктов не является на 100 процентов эффективным.

Факт того, что большое разнообразие, быстрое распространение и высокий уровень опасности,

## УДОБСТВО ИСПОЛЬЗОВАНИЯ – сравнение по количеству шагов и затраченному времени на выполнение общих задач

Задача	McAfee Total Protection for Enterprise	Sophos Endpoint Security and Control 7.0	Symantec Client Security 3.1
Инсталляция продукта и разворачивание на конечных точках	120 шагов 39 мин 27 сек	39 шагов 20 мин 43 сек	93 шага 26 мин 55 сек
Синхронизация с Active Directory	16 шагов 57 сек	11 шагов 33 сек	Нет такой функции
Определение не обновленных компьютеров	9 шагов 1 мин 5 сек	0 шагов сразу	2 шага 10 сек
Определение компьютеров не соответствующих политиками безопасности	9 шагов 39 сек	0 шагов сразу	Нет такой функции
Поиск незащищенных компьютеров	10 шагов 59 сек	8 шагов 12 сек	5 шагов 1 мин 12 сек
Задание новой политики для группы управляемых компьютеров	9 шагов 47 сек	3 шага 7 сек	3 шага 12 сек
Задание изменения политики для группы компьютеров	9 шагов 47 сек	4 шага 9 сек	3 шага 12 сек
Создание отчета обо всех обнаруженных вирусах за последние 24 часа на одном компьютере	7 шагов 41 сек	5 шагов 15 сек	9 шагов 1 мин 2 сек
Задание полного сканирования системы включая сканирование на нежелательные приложения	13 шагов 1 мин 21 сек	9 шагов 20 сек	13 шагов 37 сек
Авторизация трех нежелательных приложений для всех компьютеров	21 шаг 1 мин 52 сек	12 шагов 40 сек	9 шагов 39 сек
Защита новых компьютеров	7 шагов 1 мин 31 сек	14 шагов 1 мин 2 сек	7 шагов 1 мин 28 сек
Авторизация доступа к Интернет одного приложения	15 шагов 1 мин 17 сек	6 шагов 10 сек	23 шага 1 мин 49 сек
Блокирование запуска известных типов неавторизованных приложений	14 шагов 1 мин 9 сек	6 шагов 16 сек	Нет такой функции
Настройка HIPS (поведенческий блокиратор)	14 шагов 1 мин 26 сек	11 шагов 42 сек	Нет такой функции
Настройка частоты обновлений	9 шагов 39 сек	11 шагов 37 сек	7 шагов 27 сек
Авторизация нового патча приложения	20 сек 1 мин 49 сек	11 шагов 36 сек	Нет такой функции

которые несут в себе современные информационные угрозы, говорит нам о том, что мы должны были найти примеры вредоносных и просто нежелательных приложений, которые не смог бы определить ни один из тестируемых продуктов. Однако через защиту от Sophos (спасибо поведенческому анализатору Behavioral Genotype) не смогли пройти 88 из 100 угроз «нулевого дня». На тринадцать больше, нежели определили продукты Symantec и McAfee.

Кроме того, продукты дифференцировались по тому, каким именно образом они блокировали угрозы. В большинстве случаев

продукты блокировали вирусы в режиме on-access (на лету), что является в общем идеальным поведением блокираторов. С другой стороны, много вирусов и программ-реклам не проводят опасных действий до той поры, пока они не будут установлены на компьютер и запущены. В случаях, когда сигнатурный метод определения вирусов был неэффективен, мы смотрели насколько поведенческие блокираторы смогут смягчить ущерб «удачной» атаки.

Продукты также сравнивались по тому, как именно используются в них технологии поведенческой блокировки вредоносных кодов, то есть технологии HIPS. Sophos,

в частности, интегрировал HIPS непосредственно в движок самого антивируса, объединив таким образом в одном агенте на рабочей станции все возможные виды определения угроз. McAfee интегрировал HIPS в клиентский бренд-мауэр, не объединяя его с антивирусом. Это, в свою очередь, приводит к тому, что антивирус и бренд-мауэр несколько дублируют функции друг друга. Symantec предлагает лишь частичный функционал HIPS, интегрированный в антивирус.

Так как по результатам тестирования ни один продукт не дал 100-процентной защиты, то на первый план выходит рассмотрение таких функций продуктов, как мониторинг, управление и контроль за исполнением корпоративных политик безопасности. В этой области различия в продуктах начинают проявлять себя еще с момента начала инсталляции. Для того чтобы получить максимальную отдачу от тестирования и развертывания, мы установили все возможные компоненты защиты и управления каждого из продуктов в небольшой сети из 5-ти клиентских компьютеров на базе Windows XP.

Инсталляция Sophos Endpoint Security and Control 7.0 представляет собой последовательный процесс, на основе интерфейсов в стиле «помощников» (wizard-style), в которых используются логически правильные значения по умолчанию. Инсталляция и развертывание Sophos обошлись всего в 39 шагов и 20 минут на весь процесс. Если сравнить с другими рассматриваемыми пакетами то, например, McAfee Total Protection for Enterprise потребовал 120 иногда совершенно очевидных шагов и более 39 минут на инсталляцию. Symantec Client Security 3.1 потребовал 93 шага и почти 27 минут на инсталляцию. Важно отметить тот факт, что в крупном бизнесе компании часто снимают с себя некоторую часть головной боли по распределенной инсталляции за счет создания образов, которые уже включают некоторый, специфичный для компании набор конфигураций и правил, созданный при первой инсталляции.

По другую сторону инсталляции находится каждодневный процесс

СКОРОСТЬ СКАНИРОВАНИЯ— сравнение по скорости сканирования			
Задача	McAfee Total Protection for Enterprise	Sophos Endpoint Security and Control 7.0	Symantec Client Security 3.1
Сканирование диска C: (вирусов нет)	9 мин 25 сек	6 мин 47 сек	5 мин 14 сек
Сканирование диска C: (повторное сканирование на проверку качества кэширования)	9 мин 29 сек	3 мин 22 сек	2 мин 5 сек
Сканирование по запросу (папка содержит 1636 файлов, всего 392 МБ – без архивов и вирусов)	16 сек	9 сек	18 сек
Сканирование «на лету» (копирование и вставка той же папки)	30 сек	29 сек	50 сек

управления, создания отчетов и генерации тревог, который в совокупности и создает конечную стоимость владения системой защиты. Мы сделали заключение, что продукт Sophos по многим параметрам превосходит рассмотренные продукты от Symantec и McAfee за счет более простого процесса использования, который в итоге приведет к серьезной экономии ресурсов, затрачиваемых на систему защиты, по такому параметру как стоимость владения. Сложность информационных систем крупных компаний рождает требование к более простым и наглядным средствам управления. Достойная с точки зрения простоты использования и широты возможностей система станет хорошим фундаментом для реализации корпоративных политик безопасности и построению ИТ-процессов. С этой точки зрения продукт McAfee дает администратору максимум гибкости в конфигурировании системы безопасности, но цена такого подхода – трата слишком большого времени и других ресурсов на освоение продукта и прилаживание его к изначально выдвинутому к системе безопасности требованиям, в реализацию которых собственно и вкладывались деньги.

И наконец, следует остановиться на таких параметрах, как скорость работы и система обновления. Рассмотренные продукты в случае использования максимальных возможностей системы сканирования, могут серьезно загружать рабочие станции, поэтому оптимизация процесса сканирования, также весьма важный параметр. И продукт Symantec и Sophos имеют в наличии систему

кэширования, которая в итоге положительно сказалась на общей скорости сканирования.

С точки зрения системы обновления, которая должна влиять на устойчивость системы защиты от новых информационных угроз, все три компании показали удовлетворительные результаты по скорости обновления локальных антивирусных баз на конечных точках с корпоративного сервера обновлений, и по скорости получения обновлений с центрального сервера. В прошлом, скорость обновления была серьезным индикатором, по которому можно было легко дифференцировать продукты. Но с тех пор как McAfee и Symantec «подтянулись» и стали выпускать ежедневные обновления, сегодня в этом плане продукты отличаются мало. Однако Sophos предоставляет обновления несколько раз в день, что в сочетании с быстрой реакцией лабораторий производителя на новые угрозы, в итоге серьезно повышает адекватность системы защиты.

### Вердикт

Каждая крупная компания имеет свои собственные уникальные отличия. Для тех компаний, которые в первую очередь обращают внимание на прозрачность и удобство интерфейса, продукт Sophos будет хорошим выбором, далеко опережающим Symantec и McAfee в вопросах простоты использования и ежедневного управления защитой, без потери качества и какой-либо функциональности. Глубокие и всесторонние отчеты McAfee и широкие возможности по конфигурирова-

нию будут востребованы в некоторых крупных компаниях, но многие компании найдут этот продукт слишком сложным в использовании и слишком громоздким. Symantec, так же как и другие продукты представляет полную защиту конечных точек, однако его методы строятся на основе уже устаревших архитектур управления, которые никогда не были простыми в использовании и не давали требуемой администратору гибкости в настройках.

## McAfee Total Protection for Enterprise

Пакет программ McAfee Total Protection for Enterprise это комплексное решение специально созданное для очень больших компаний. Он предлагает целый набор опций конфигурирования и наиболее гибкую систему развертывания среди всех рассмотренных продуктов. Однако мы сделали заключение, что продукт слишком труден в инсталляции и использовании. Как и другие продукты, которые мы тестировали, данный пакет предлагает в общем эффективную, но не идеальную защиту против тех информационных угроз, на которых мы проводили тестирование.

### Начало

Инсталляция пакета McAfee Total Protection for Enterprise это слишком трудная и длительная работа. Сам пакет включает в себя множество различных продуктов McAfee, которые могут быть не совсем совместимыми между собой. Например, мы инсталлировали текущую версию 3.6.1 модуля администрирования центрального сервера - ePolicy Orhestrator (ePO). Однако эта версия связана с клиентской версией агента 3.5.5 (Common Management Agent), который в свою очередь несовместим с последним антивирусным программным обеспечением (VirusScan Enterprise 8.5i), которое собственно и должно защищать рабочие станции. После сканирования массы сопроводительной документации нам в итоге пришлось обратиться к поиску через Google для разрешения проблемы. В итоге мы нашли и скачали последние обновления программно-

го обеспечения, с помощью которых и закончили инсталляцию.

В итоге процесс инсталляции McAfee занял 120 шагов, что можно сравнить со всего 39-ю шагами по инсталляции Sophos. У McAfee нет wizard-системы, которая бы помогала провести пошаговую инсталляцию. В итоге многие вещи приходилось делать вручную, как например добавление и обновление компонент пакета и встраивание их в единую систему управления ePO. Вместе с пакетом Total Protection for Enterprise мы инсталлировали ePO сервер, пакет VirusScan Enterprise 8.5i (антивирусный клиент), модуль Anti-Spyware 8.5 (добавка к антивирусному модулю, защита от программ-шпионов), и Host Intrusion Prevention 6.1 (отдельный модуль с брандмауэром и клиентом HIPS).

McAfee ePO поддерживает интеграцию с Active Directory, что позволяет администраторам автоматически синхронизировать деревья AD с консолью управления ePO. Эта опция может быть особенно важна в случаях использования больших корпоративных сетей на базе технологий Microsoft.

McAfee Total Protection for Enterprise поддерживает такие операционные системы как Windows XP, Windows 2003, Windows 2000, Windows NT 4.0 и NetWare. McAfee также предлагает набор различных компонент для Macintosh и Linux, но они продаются отдельно и могут управляться с центральной консоли лишь частично.

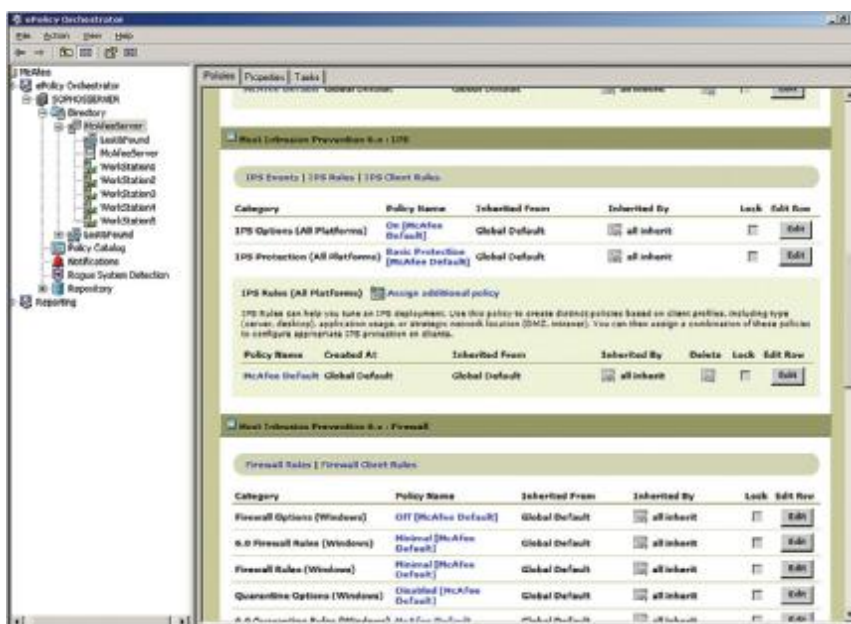
### Удобство использования

Администраторы используют консоль ePO для решения всех возникающих проблем, в частности для развертывания агентов, управления политиками безопасности, задания тревог и генерации отчетов. Администратор может также подготовить к исполнению несколько наиболее общих задач, таких как обновление конечных точек, создание отчетов, и применение новых политик безопасности в сети.

Во время тестирования мы обнаружили тот факт, что консоль ePO намного трудней в применении нежели консоль Sophos Enterprise

Console или Symantec System Center. Было сложно найти важную информацию быстро и, в отличие от Sophos, в данной консоли нет индикационной панели, которая бы наглядно демонстрировала наиболее важные параметры. Более того, «сборный» тип архитектуры консоли ePO приводит к мысли о том, что пакет McAfee это некий сбор плохо интегрированных компонент, нежели целостный пакет. Пока одни пользовательские интерфейсы использовали стандартные компоненты, другие требовали установки ActiveX в Internet Explorer или требовали развернуть на компьютере среду исполнения Java. В итоге, во время одной сессии

настройках политик продемонстрирована в несколько более обескураживающем виде, нежели в Sophos или Symantec. Например, конфигурационные опции HIPS распределены по 15-ти файлам, уложенным в 4 категории. Что приводит к необходимости сделать довольно большое число шагов для того, чтобы настроить весьма обыденные вещи. Однако для очень больших организаций, где существуют разные команды менеджеров, управляющих сегментами сети, в которой могут быть десятки тысяч компьютеров, такая гибкая система конфигурирования может подойти. Например, консоль ePO дает администраторам возможность задавать



Настройка политик безопасности через консоль ePO представляется весьма трудной задачей, так как требуется работать с большим количеством конфигурационных файлов и опций, объединенных в неповоротливый интерфейс

конфигурирования нам пришлось установить виртуальную машину Sun Java J2RE, которая затем потребовала перезагрузки нашего основного сервера.

Настройки управления политиками безопасности в ePO объединены занимательным образом. С одной стороны, такая группировка хорошо демонстрирует наследственную модель процедур развертывания политик через корпоративные группы компьютеров, и кроме того, консоль демонстрирует весьма обширный набор управляемых настроек для приложений разного типа. С другой стороны информация о текущих

номера сетевых портов, которые будут использоваться всеми компонентами пакета McAfee. Кроме того консоль представляет собой неплохую систему обнаружения новых конечных точек или точек, чья конфигурация не соответствует заданной.

McAfee также продемонстрировал мощную систему отчетности. Существует набор уже готовых отчетов и кроме этого администраторы могут получать свои уникальные отчеты напрямую создавая SQL-запросы. Более того, администраторы могут использовать систему Crystal Reports 8.5, для создания новых отчетов. С другой стороны

текущий интерфейс генерации отчетов слишком перегружен и труден в освоении. Будьте готовы к тому, что придется приложить некоторые дополнительные усилия для того, чтобы вытянуть из McAfee нужную информацию.

### Эффективность

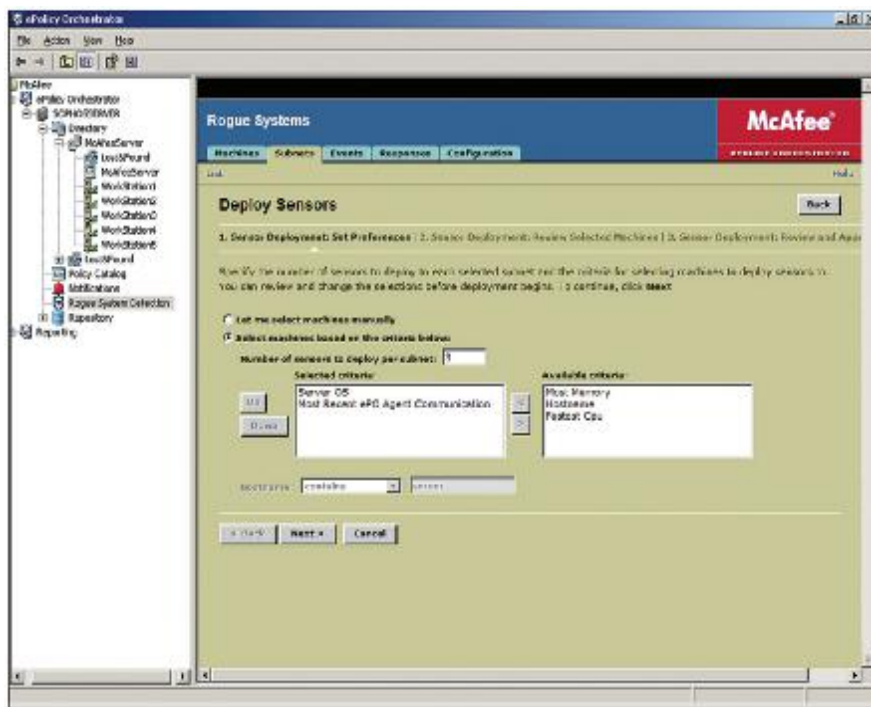
В основном McAfee удовлетворил наши ожидания в борьбе против информационных угроз, на которых мы проводили тестирование. Совокупность обеих инсталлиро-

McAfee Host Intrusion Prevention, это полнофункциональная система защиты, объединяющая в себе брандмауэр, защиту на базе вирусных сигнатур и поведенческий блокиратор. Так же как и антивирус Sophos, McAfee предлагает возможность блокирования запуска неавторизованных приложений. Однако реализация этого механизма в McAfee несколько неудобна тем, что в отличие от Sophos, требует запрещать или давать доступ на запуск для каждого приложения вручную. В

характеристики McAfee улучшились, и хотя он обошел по скорости Symantec, все равно антивирус Sophos был быстрее.

### Заключение

Пакет программ McAfee Total Protection for Enterprise можно назвать хорошим выбором для защиты конечных точек с очень гибкой конфигурацией. Компании, которые имеют должный штат грамотных специалистов по безопасности и четко определенные политики безопасности могут остановить свой выбор на McAfee. Однако компанию, которая находится в поиске более простого решения, такой продукт может привести в уныние.



McAfee Rogue System Detection дает администраторам конфигурировать сетевые датчики в разных подсетях корпоративной сети для детектирования новых или неподдерживаемых систем

ванных систем VirusScan Enterprise и Host Intrusion Prevention вместе смогли обнаружить 75 из 100 новых и неизвестных угроз, столько же сколько и Symantec, но меньше чем у Sophos – 88.

Кроме этого McAfee проделал хорошую работу по выявлению уже известных угроз. Далее, McAfee показал наилучшие среди тестируемых продуктов результаты по противостоянию программам-рекламам (adware), останавливая их работу еще в процессе инсталляции. Более того, этот продукт неплохо показал себя в противостоянии угрозе по переполнению буфера.

Sophos, в свою очередь, используется уже готовый исходный список приложений, который можно использовать для блокировки приложений.

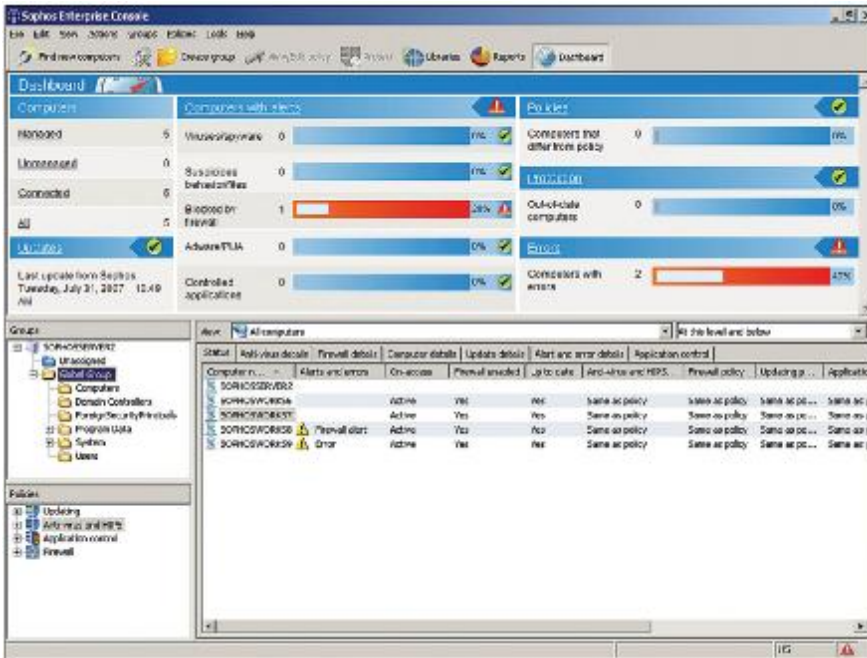
В нашем тесте на скорость продукт McAfee сильно отставал от Symantec и Sophos. При сканировании системного диска по запросу, McAfee потребовалось 9 мин 25 сек, на 4 минуты больше чем для этого потребовал Symantec. Более того, из тестируемых продуктов только McAfee не имел систему кэширования, следовательно второе сканирование того же диска заняло у McAfee почти такое же количество времени, что и первое. Однако в режиме сканирования «на лету» скоростные

## Sophos Endpoint Security and Control 7.0

Sophos Endpoint Security and Control представляет собой неплохую сборку технологий, которые сочетают в себе серьезную защиту для конечных точек с развитыми возможностями управления и простым интерфейсом. Последовательный процесс инсталляции вместе с интуитивно понятным пользовательским интерфейсом и индикационной панелью уменьшают головную боль в процессе управления безопасностью. Кроме этого стоит отметить наилучшие среди трех тестируемых продуктов результаты по определению новых и неизвестных вирусов. С другой стороны во время тестов мы определили, что возможности Sophos по генерации отчетов сравнимы с другими продуктами лишь на минимальном уровне.

### Начало

Что касается простоты и удобства процесса инсталляции, то продукт Sophos Endpoint Security and Control оставляет все другие рассмотренные продукты далеко позади. Все компоненты Sophos собраны в единый хорошо интегрированный пакет, инсталляция и развертывание которого происходят быстро и без лишней головной боли. Развертывание Sophos в нашей тестовой лаборатории заняло всего 20 минут, из которых основная масса времени ушла на закачивание с сайта Sophos последних об-



В Sophos Enterprise Console реализована индикаторная панель, которая позволяет быстро получать актуальную информацию о системе

новлений ПО и свежих антивирусных баз. Для сравнения и Symantec и McAfee потребовали многое установить в ручном режиме, что в свою очередь потребовало много времени и серьезных знаний в том, как правильно устанавливать продукт. Если сравнивать с Sophos, то Symantec потребовал в два раза, а McAfee в три раза больше шагов по установке.

Во время установки мы смогли найти рабочие станции и сервера в автоматическом режиме, используя Microsoft Active Directory. Также как и в McAfee Total Protection for Enterprise в Sophos поддерживается как однократное считывание структуры Active Directory для импорта в консоль, так и постоянная синхронизация. С автоматической синхронизацией администраторы могут создать правила, по которым на новые станции, появляющиеся в дереве AD, будет автоматически устанавливаться необходимое ПО защиты, без какой-либо дополнительной работы в консоли управления.

Sophos Endpoint Security and Control предлагает защиту для самого широкого круга операционных систем, большего чем у Symantec и McAfee, и покрываемого единой лицензией. Он поддерживает Windows 95 или позже (включая Windows Vista), Mac OS X 10.2 или

позже, серверные операционные системы Windows Server 2000 и 2003, а также Netware, Linux, Unix, NetApp Storage Systems и Windows Mobile. Брандмауэр Sophos поддерживает такие платформы как Windows 2000 и позже.

### Удобство использования

В рамках данного тестирования продукт Sophos был единственным, в котором вся работа администратора проводится из одной унифицированной консоли. Консоль Sophos Enterprise Console собирает информацию со всех компонент защиты и демонстрирует ее в удобном для пользователя интерфейсе.

Центральным местом консоли можно назвать индикаторную панель, в которой отображается суммарный отчет по той информации, которая востребована администратором в первую очередь. В ней можно увидеть факт появления новых вирусов, компьютеров, на которых локальные настройки не совпадают с заданной политикой, общую сумму управляемых и не управляемых с консоли рабочих станций и т.д. Если сравнить интерфейс Sophos с Symantec или McAfee, то можно сделать вывод, что индикаторная панель Sophos действительно весьма удобный компонент. Например, в продукте McAfee быстро

получить аналогичную обобщенную информацию о текущем состоянии быстро не получится.

Мы также использовали консоль чтобы создавать, настраивать и распространять политики безопасности. Консоль Sophos поддерживает разделение политик безопасности на политики для антивируса/HIPS, брандмауэра, системы управления приложениями и системы обновления. Таким образом, конфигурирование каждой конечной точки в группах через такие разделы политик безопасности в итоге превратилось в очень простую задачу.

В наших тестах на удобство использования, выполнение большинства наиболее общих административных задач в Sophos в среднем занимало меньше времени и шагов, нежели в Symantec или McAfee. Ярким контрастом между тестируемыми продуктами было то, что в консолях Symantec и McAfee последовательность шагов по выполнению той или иной задачи была намного труднее, была замысловата и неочевидна.

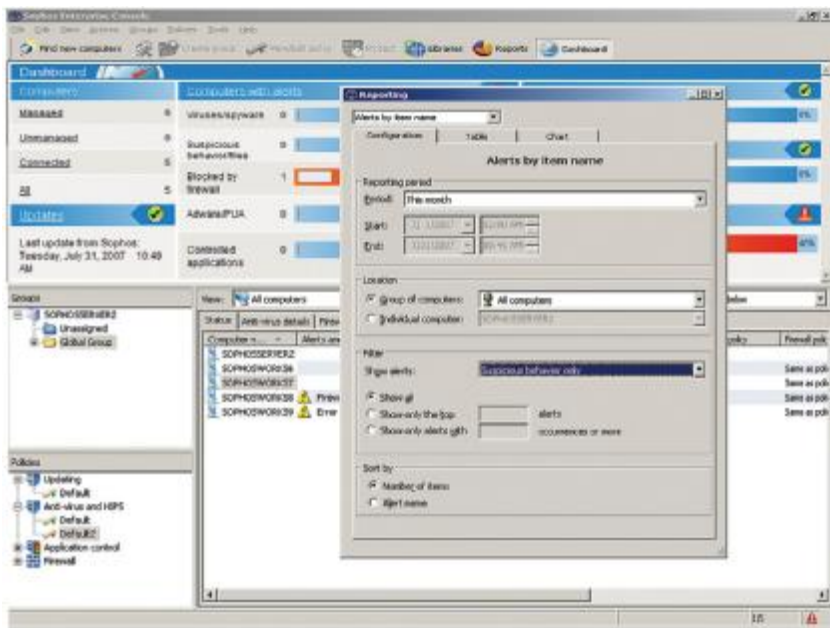
Наконец, система отчетов Sophos Endpoint Security and Control была адекватной, но не настолько всесторонней, как в других пакетах. Консоль Enterprise Console предлагает встроенного «помощника» для генерации отчетов по некоторому набору шаблонов в графическом виде или в табличном. Sophos также может создавать ежедневные, еженедельные и ежемесячные отчеты по текущей ситуации в сети и новым угрозам. Кроме того имеется функциональность по удалению из Базы Данных устаревшей информации. Однако мы бы хотели увидеть более гибкий функционал системы отчетов на том уровне, который обычно требуется для крупных компаний. Такие компании могут иметь требования к получению информации несколько большей, нежели может предоставить текущий готовый набор, редактировать который нельзя.

Консоль управления Sophos позволяет также проводить последовательные действия по защите от программ-реклам, и другим нежелательным приложениям (PUA). Она может показать те PUA,

которые были обнаружены во время удаленного сканирования антивирусом или в логах брандмауэра, что намного упрощает администратору процесс создания политик, которые регулируют работу с PUA. Например, полное сканирование в системе может выдать в результате полный список найденных нежелательных приложений, и по нему администратор может авторизовать каждое

Продукт Sophos показал себя наилучшим образом в наших тестах на эффективность защиты против новых и неизвестных угроз в сравнении с результатами тестов Symantec и McAfee. Используя комбинацию сигнатурного поиска и поведенческого блокиратора HIPS Sophos смог определить 88 из 100 угроз, на 13 больше чем Symantec и McAfee.

такую программу в режиме сканирования «на лету». Но сразу после инсталляции Sophos определил эту программу при сканировании по запросу. Кроме этого, все наши остальные угрозы были заблокированы Sophos полностью при сканировании «на лету», включая также такую угрозу как переполнение буфера. Технология Sophos HIPS, при помощи которой определяются потенциально вредоносные действия (такие как удаление защищенных ключей реестра или попытки изменения системных файлов) помогла заблокировать эти действия, прежде чем они были выполнены.



Настройка отчетов в Sophos Endpoint Security and Control производится удобным и не сложным путем, однако нам бы хотелось большей гибкости в настройках отчетности

Если говорить о скорости, то Sophos здесь также оставил другие тестируемые продукты позади. В наших тестах на сканирование одной и той же папки в режиме «по запросу» Sophos было достаточно половины того времени, которое понадобилось Symantec и McAfee. При сканировании целиком одного диска Sophos потратил чуть больше времени, чем Symantec, но сильно опередил McAfee. Более того, в сканирующей движок Sophos, как и в Symantec, внедрен механизм кэширования, с использованием которого на вторичном сканировании можно сэкономить до 50% потраченного первоначально времени.

такое приложение к использованию, или запретить и удаленно деинсталлировать его. Кроме этого в продукт Sophos внедрена довольно мощная система управления всеми клиентскими приложениями. Администраторы могут использовать Sophos для авторизации или блокирования и легитимного ПО (не PUA или adware). Из тестируемых продуктов только Sophos обладает списком легитимных приложений, таких как P2P, модули расширения для браузеров и Интернет-пейджеров. Используя эту обновляемую Sophos базу, администраторы могут не трудиться над созданием собственных списков авторизованных или неавторизованных приложений, особенно когда производители выпускают очередные обновления и контрольные суммы файлов меняются.

## Эффективность

Основой для такой эффективности Sophos стала технология Behavioral Genotype Protection - поведенческий генотипный блокиратор. Эта технология легла в основу технологии Sophos HIPS, при помощи которой вредоносные действия приложений блокируются до того, как они будут выполнены. В некоторых случаях данный блокиратор определил угрозы, которые не определили ни Symantec ни McAfee.

Кроме этого, Sophos неплохо показал себя в определении уже известных угроз из нашего набора. Sophos был единственным антивирусом, который определил и заблокировал кейлоггер до его запуска (спасибо генотипной защите). В другом случае Sophos определил кейлоггер только после перезапуска операционной системы. В наших тестах на устойчивость к программам-рекламам (adware) Sophos не смог поймать

Sophos предоставляет антивирусные обновления в сжатом виде. Обновления Sophos приходят несколько раз в день, у других производителей они приходили не чаще чем раз в день. Более того размер обновлений Sophos удается удерживать весьма малым, что будет особенно приятно компаниям с распределенной сетевой структурой, которым с одной стороны требуется не нагружать трафик, а с другой иметь на каждой защищаемой точке все последние обновления. Sophos также обладает возможностью обновлять автоматически не только антивирусные базы, но и само программное обеспечение. У Symantec, например, такой возможности нет.

## Заключение

Пакет Sophos Endpoint Security and Control сочетает в себе высокую эффективность защиты и отличные скоростные качества, объединенные в хорошо интегри-

рованном продукте с более удобным интерфейсом, чем у Symantec и McAfee. Комбинация простоты архитектуры с высокой скоростью и эффективностью может являться сегодня наилучшим выбором в крупных компаниях, ищущих сегодня мощный и удобный в использовании продукт.

## Symantec Client Security 3.1

Пакет Symantec Client Security 3.1 представляет собой эффективный продукт с некоторыми сильными сторонами, но в нем нет такого удобства управления как в Sophos, и такой гибкости в развертывании, как в McAfee. В нашем тесте этот продукт был единственным, не поддерживающим интеграцию с Active Directory и систему управления приложениями. Кроме того возможности системы HIPS у Symantec оказались весьма ограниченными, а система управления политиками безопасности намного слабее, нежели у других представленных продуктов. С другой стороны Symantec показал себя неплохо в наших тестах на эффективность работы системы защиты, а также скоростные характеристики были весьма обнадеживающими.

### Начало

Процесс инсталляции Symantec Client Security 3.1 был сильно запутан. Несмотря на это действия по инсталляции не были столь беспорядочными и длительными, как например у McAfee. Во время инсталляции потребовалась установка нескольких программных продуктов, что обошлось в 93 шага, что сильно контрастирует с 39-ю шагами у Sophos. С другой стороны мы не смогли найти документации, в которой нормально и пошагово был описан процесс инсталляции, в результате которого можно было бы запустить пакет в режиме «по умолчанию».

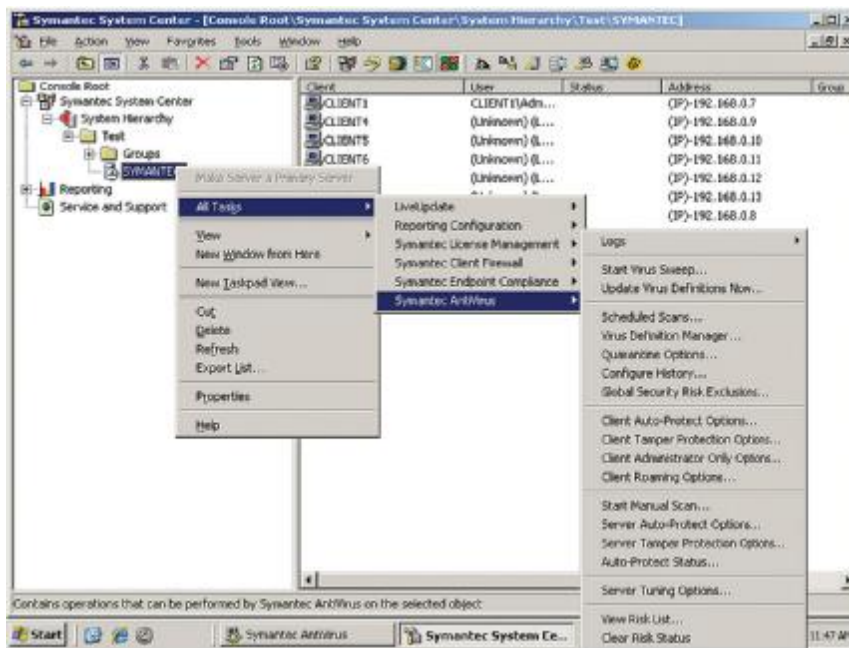
Как уже отмечалось, пакет Symantec Client Security не поддерживает Active Directory, в результате администраторы должны вручную указывать конечные точки для развертывания, используя для их поиска браузер Windows или прямой поиск по IP-

адресам. Стоит обратить внимание на то, что отсутствие поддержки Active Directory лишает администраторов такой важной возможности, как автоматическая синхронизация изменений в AD и иерархии компьютеров в консоли управления – весьма полезная функциональность в случае добавления или удаления компьютеров из сети.

Symantec Client Security поддерживает платформы Windows XP, Windows 2000, Windows 2003 и

сторону мы нашли удобным возможность задания политик для антивируса прямо из консоли Symantec System Center, а с другой стороны совсем неудобным использование другой консоли для задания политик брандмауэра.

Symantec позволяет сосуществовать разным наборам политик для антивируса и брандмауэра в рамках одного домена, посредством разделения его на серверные группы, и задания для каждой такой группы индивидуальных



*Symantec Client Security 3.1 предлагает большое количество опций для настройки окружения безопасности, однако в отличие от других продуктов здесь сложнее проследить за тем, как применяются политики безопасности*

Netware. Symantec предлагает также продукты для Linux и Mac OS, но приобретаются они отдельно и не управляются из той же консоли, из которой управляются Windows-компьютеры.

### Удобство использования

Несмотря на то, что система управления Symantec многофункциональна, она не так удобна и наглядна, как у Sophos. Система управления – Symantec System Center – представляет собой интегрированный в MMC-консоль (Microsoft Management Console) интерфейс, с помощью которого управляется антивирус и производится генерация отчетов. Кроме этого, Symantec предлагает отдельную не интегрированную в MMC консоль, для управления политиками брандмауэра. С одной

конфигураций. Каждая такая серверная группа, в свою очередь, может иметь подгруппы со своими конфигурациями. Такой многоступенчатый метод создания иерархий может быть интересен крупным компаниям, имеющим многофилиальную распределенную сетевую структуру, так как позволяет администраторам производить настройку политик только в рамках какого-то одного сегмента компании. Однако с другой стороны в Symantec в отличие от Sophos и McAfee труднее следить за итоговыми настройками компонент защиты во всей корпоративной сети. В Symantec не поддерживается именование групп политик безопасности, что не дает возможности быстро проследить за выполнением политик в группах, и делает весьма затруднительным получение информации

о том, какие именно политики были применены в группах.

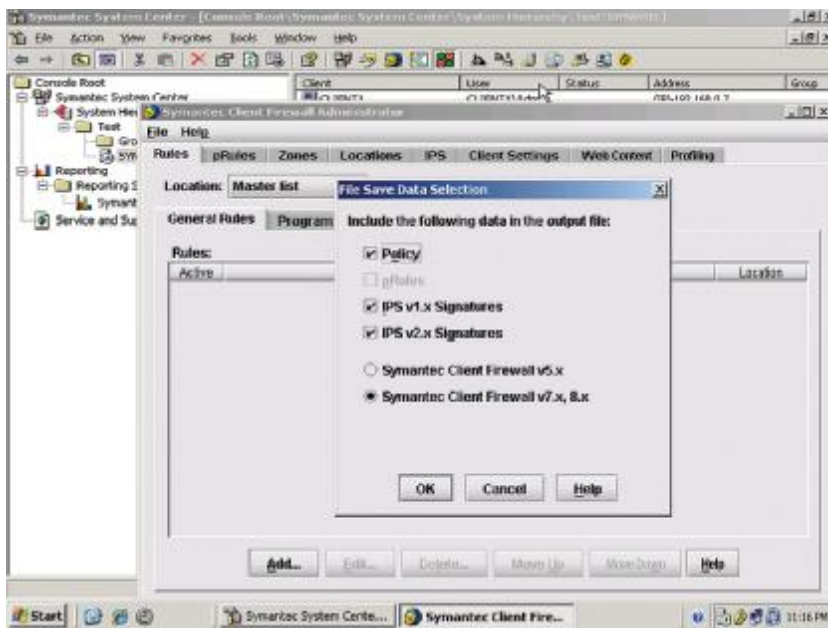
Symantec System Center предлагает набор инструментов для конфигурирования антивируса, карантина, а также получения обновлений. Кроме того существует специальная подсистема, с помощью которой можно проследить за сетевыми путями к клиентским компьютерам, по результатам работы которой можно найти самый оптимальный способ подключения клиентов к серверам. Брандмауэр позволяет администраторам следить за сетевой активностью приложений, идентифицируя их по контрольным суммам и версиям файлов (в комбинации директория-имя файла). Однако в отличие от Sophos и McAfee продукт Symantec не позволяет блокировать запуск нежелательных приложений (VoIP, Интернет-пейджеры и т.д.).

Возможности генерации отчетов в Symantec довольно широки. Зкладка «Home» в диалоге отчетов дает неплохой отчет о текущей активности, например о детектировании новых угроз и суммарного количества обнаруженных и вылеченных вирусов. Богатый набор predefined отчетов поможет найти информацию об истории сканирования, отражений угроз и состоянии «здоровья» конечных защищаемых точек во всей сети. В плане гибкости, к сожалению, администраторы ограничены только возможностью создания заданий на генерацию отчетов по расписанию.

### Эффективность

В наших тестах на новые угрозы и неизвестные вирусы пакет Symantec показал себя вполне неплохо. С использованием сигнатурного подхода и распознавания на основе шаблонов Symantec смог определить 75 из 100 вирусов, столько же сколько и McAfee, но меньше чем 88 у Sophos. С использованием обновленной антивирусной базы, выпущенной Symantec через две недели после нашего первого теста, антивирус смог дополнительно определить еще 3 вируса из нашего набора.

Кроме этого Symantec неплохо показал себя в определении уже



Администратор брандмауэра от Symantec не интегрирован в консоль управления антивирусом, что требует некоторого напряжения при создания политик управления брандмауэром

известных вирусов из того набора, на котором мы производили тесты. Антивирус Symantec также был единственным, из протестированных нами, кто смог также определить и заблокировать кейлоггер еще на этапе его инсталляции. Однако в тестах защиты от программ-реклам, антивирус Symantec был единственным из протестированных, кто не смог противостоять инсталляции такой программы. Далее, антивирус Symantec был единственным из протестированных антивирусов, у которого не было технологии поведенческого блокиратора или HIPS. С другой стороны Symantec остановил нашу попытку переполнения буфера.

Symantec также неплохо показал себя в тестах на скорость работы. В тестировании скорости сканирования системного диска Symantec показал лучший результат - 5 мин 14 сек, на полторы минуты быстрее, чем его ближайший соперник по скорости – Sophos. Второе сканирование того же диска прошло за 2 мин 5 сек, или на 60% быстрее, чем первое сканирование, за счет технологии кэширования. К сожалению, в тестах на скорость работы в режиме «на лету» Symantec оказался на 50% медленнее, чем и Sophos и McAfee при обработке операции по копированию папки.

Symantec в последнее время стал выпускать обновления ежедневно, что повышает степень актуальности защиты конечных точек. Однако Symantec не позволяет автоматически обновлять само программное обеспечение, как это делают другие.

### Заключение

Symantec Client Security 3.1 представляет собой вполне адекватную защиту против многих разновидностей информационных атак, и будет неплохим выбором для крупных компаний, имеющих достаточно времени, чтобы разобраться с его интерфейсами управления.

## Что означает наш рейтинг

Мы провели инсталляцию каждого из рассматриваемых продуктов в нашей тестовой сети на базе Windows 2003 (с использованием Active Directory) на сервере и 5-ти клиентских компьютеров Windows XP. После настройки мы подвергли сеть воздействию различных видов атак – от известных вредоносных программ до новых и малоизученных видов угроз для того,

чтобы понять, как работают такие функции продуктов как поведенческие блокираторы, брандмауэры, и другие средства защиты. Мы также выполнили типичные административные задачи, такие как добавление новых компьютеров в сеть, предоставление исключений отдельным приложениям на индивидуальных ПК, а также изучили действия тревог и отчетность. Затем мы оценили работу каждого продукта по четырем следующим категориям.

#### **Инсталляция и развертывание.**

Оценивается опыт установки ПО сервера и панели управления, а также внедрения ПО безопасности конечных точек на машинах клиентов и серверах в сети. Мы отдали предпочтение полностью интегрированным продуктам, имеющим простые подсказки ("мастера") инсталляции, а также тем продуктам, которые автоматически распознавали новые компьютеры через службу каталогов Active Directory, систему Windows NetBIOS или по IP-адресам.

**Удобство и наглядность.** Оценивается простота первичной настройки продукта, а также его последующего использования. Мы проверяем отдельные задачи, такие как задание конфигурации «по умолчанию» для конечных

точек, создания рабочего пространства, запуск сканирования, конфигурирование брандмауэра, удаление следов заражения, и авторизация потенциально нежелательных приложений. Кроме этого мы также проверяли задачи, выполняемые обычно конечными пользователями: сканирование файлов, полученных по электронной почте или другим способом, загрузка обновлений на мобильные компьютеры, находящиеся за пределами корпоративной сети, и получение информации о тех приложениях, которые были по разным причинам блокированы. Мы также давали дополнительные очки тем продуктам, которые хорошо ориентированы специально для работы в крупных компаниях. Это может быть такая характеристика как интеграция с Active Directory или возможность определения места подключения станции к сети.

**Эффективность.** Эффективность оценивается с точки зрения качества защиты как от известных так и от новых угроз. Для теста сигнатурных методов мы использовали широкую базу вредоносных программ, таких как вирусы и их разновидности, программы-шпионы, программы-рекламы и другие нежелательные приложения. В тестах на качество проти-

востояния угрозам «нулевого дня» мы тестировали возможности систем защиты по остановке или минимизации ущерба от новых и неизвестных вирусов, программ-шпионов и других программ. Мы тестировали антивирусы, anti-spyware, брандмауэры, поведенческие блокираторы, защиту от переполнения буфера и других вредоносных действий. Мы применяли базовые настройки, а также тестировали продукты с использованием их настроек по умолчанию. Для обеспечения равных условий мы применяли в тесте экземпляры вредоносного ПО из собственной коллекции, не используя образцы от производителей.

**Производительность.** Оценивается, насколько хорошо каждый продукт минимизирует воздействие на пользователей при выполнении распространенных задач, таких как сканирование по доступу, полносистемное сканирование как на чистых машинах, так и на компьютерах, зараженных рекламным ПО и вирусами, а также обновление сигнатур. ▲



Independent evaluations of technology products

Contact: [inquiry@cascadialabs.com](mailto:inquiry@cascadialabs.com)

[www.cascadialabs.com](http://www.cascadialabs.com)

# SOPHOS

*Этот сравнительный обзор, проведенный независимо компанией Cascadia Labs в июле 2007 года, финансировался компанией Sophos. Компания Cascadia Labs стремится проводить объективный анализ каждого продукта на основании практического тестирования в собственной лаборатории, при этом предоставляя каждой компании, чья продукция тестируется, возможность участия с использованием информации, предоставленной Cascadia Labs для плана тестирования, а также предоставления обратной связи по заключениям после проведенного тестирования*