

Безопасность конечных точек для компаний малого бизнеса

В этом обзоре:

- McAfee Active VirusScan SMB (версия для малого бизнеса) (страница 3)
- Sophos Computer Security Small Business Edition (SBE) 2.0 (версия для малого бизнеса) (страница 5)
- Symantec Client Security 3.1 (страница 7)

Хотя уже давно не является новостью то, что компании регулярно сталкиваются с все новыми угрозами безопасности их сетям и компьютерам, однако, по-прежнему нет полной ясности относительно того, что им следует делать для противодействия этим угрозам. Большинство тех, кто принимает решения, знают, что им требуется антивирусное программное обеспечение для защиты настольных систем – однако сегодняшнее распространение все более сложного вредоносного программного обеспечения означает, что одного такого ПО уже недостаточно. В действительности, только комплексный подход, включающий также технологии против шпионского ПО, поведенческие анализаторы и персональные брандмауэры, способен обеспечить полную безопасность для конечных (endpoint) точек.

Правильное соединение указанных компонентов является особо сложной задачей для малого бизнеса.

Идеальный программный комплект для обеспечения безопасности

Идеальным комплектом программ для обеспечения безопасности малого бизнеса является тот, который предоставляет широкий набор эффективных средств защиты всех соответствующих конечных точек – другими словами, всех ноутбуков, рабочих станций и серверов, работающих в ОС Microsoft Windows и все чаще в ОС Mac OS X.

С одной стороны, этим компаниям требуется более централизованная наглядность и координация в сравнении с теми функциями, что в большинстве случаев могут предложить автономные, ориентированные на потребителя продукты.

Защита должна предохранять от всего спектра угроз, включающего не только известные вирусы, но также и новые атаки, использующие уязвимости операционных систем и приложений (также известные как «угрозы нулевого дня»); новые варианты известных вирусов; а также потенциально нежелательные приложения (ПНП), включая рекламное и шпионское программное обеспечение.

С другой стороны, эти компании редко имеют время и способность для управления сложными программными решениями, рассчитанными на крупные корпорации.

Идеальный программный комплект должен также легко устанавливаться и конфигурироваться, с удобными и практичными настройками по умолчанию, не требующими особых усилий для обеспечения полной защиты.

Более того, управление и мониторинг программного комплекта должны быть простыми, чтобы возникшие вдруг из-за невнимательности устаревшие сигнатуры или машины, не удовлетворяющие соответствующим требованиям, не приводили к возникновению брешей в защитной оболочке компании (в конечном счете, решение по безопасности, сконфигурированное ненадлежащим образом или плохо поддерживаемое, не сможет обеспечить надежную защиту). Администраторы должны иметь возможность планировать процессы сканирования и следить за статусом защиты, при этом конечные пользователи должны иметь доступ к интерфейсу сканирования «по доступу» (on-access), который будет предупреждать их об опасностях и угрозах в режиме реального времени.

И, последнее, идеальный комплект безопасности объединяет эти способности в полезный, легко устанавливаемый пакет на каждую конечную точку – при наименьших требованиях к процессору и памяти компьютеров, чтобы не влиять на основные бизнес-задачи.

Оцениваемые программные комплекты безопасности

Поставщики программного обеспечения по системам безопасности предлагают много вариантов на выбор: одно-функциональные и интегрированные продукты; комплекты, ориентированные на потребителей, малый бизнес или крупные предприятия; а также ПО, которое вы сами можете настраивать в своей сети или то, которое управляется извне.

компании McAfee, Sophos и Symantec нацеливают эти свои продукты на малый бизнес. Оцененные нами комплекты содержат интегрированную защиту от вирусов, шпионского программного

РЕЙТИНГОВАЯ ТАБЛИЦА

Категория	McAfee Active VirusScan SMB Edition	Sophos Computer Security SBE 2.0	Symantec Client Security 3.1
Установка и внедрение	▲▲	▲▲▲▲▲	▲
Удобство и управление	▲▲▲	▲▲▲▲	▲▲
Наглядность	▲▲▲	▲▲▲▲	▲▲▲
Эффективность (на основе сигнатур)	▲▲▲▲	▲▲▲▲	▲▲▲▲
Эффективность (угрозы нулевого дня)	▲▲▲	▲▲▲▲	▲▲
Производительность	▲▲▲	▲▲▲	▲▲
ОБЩАЯ ОЦЕНКА	▲▲▲	▲▲▲▲	▲▲
Краткий обзор	Малым предприятиям будет сложно установить и конфигурировать отдельные компоненты – эффективность комплекта была продемонстрирована способностью находить некоторые настроечные файлы рекламного ПО.	Идеально подходит для малого бизнеса, продукт обеспечивает отличную защиту, включая превосходную поведенческую защиту, легкую установку и интуитивное управление.	Хотя защита от большинства известного вредоносного ПО была сравнима с другими продуктами, мы не думаем, что типичное малое предприятие выберет данный продукт – из-за его сложности.
Поддерживаемые платформы	Windows NT, 2000, XP, 2003	Windows 98, Me, 2000, XP, 2003, Mac OS X	Windows 2000, XP, 2003
Техподдержка	круглосуточно	круглосуточно	в рабочее время
Цена для 5 пользователей в год		269 долл. США	320 долл. США

Обозначения: ▲ - плохо ▲▲ - удовлетворительно ▲▲▲ - средне
▲▲▲▲ - хорошо ▲▲▲▲▲ - отлично

обеспечения, а также «угроз нулевого дня». Мы не рассматривали продукты или компоненты, которые каждая из вышеуказанных компаний предлагает для сканирования входящей и исходящей электронной почты на уровне почтового сервера – данная функция будет полезна только для тех компаний, которые сами поддерживают свои серверы электронной почты, такие, к примеру, как Exchange Server.

Каждый оцененный продукт продается по подписке. Вы платите минимум за пять пользователей и минимум за один год с получением периодических обновлений, что гарантирует защиту от появляющихся новых угроз. Продукты от McAfee и Sophos имеют круглосуточную техподдержку; в случае с Symantec такой вариант круглосуточной поддержки предлагает платно. Каждый из указанных программных комплектов позволяет устанавливать компонент по управлению на одном существующем сервере в сети.

Наши выводы

Как уже объяснялось ранее, два фактора являются важными для программного комплекта безопасности конечных точек, ориентированного на малые предприятия. Во-первых, такой комплект должен обеспечивать эффективную защиту от целого ряда угроз. Во-вторых, комплект должен легко устанавливаться и через какой-то промежуток времени подвергаться администрированию.

Когда мы тестировали продукты от McAfee, Sophos и Symantec в своей лаборатории безопасности, мы обнаружили существенные различия между поведением этих продуктов.

используя для этого типичную конфигурацию сети для малого бизнеса, которая состоит из сервера MS Windows 2003, десяти рабочих станций Windows XP Professional и компьютера Apple Macintosh,

Разница стала очевидной, как только мы стали устанавливать продукты. Sophos Computer Security SBE 2.0 применяет прямой, основанный на «мастере» интерфейс, который выбирал приемлемые настройки по умолчанию, а на установку и внедрение продукта у нас ушло всего 15 минут. На другом конце спектра – продукт Symantec Client Security 3.1, который поставил в процессе установки в три раза больше вопросов, чем продукт от Sophos, – при этом большинство вопросов было ориентировано, в основном, только на случаи применения в крупных предприятиях, но не для малого бизнеса, состоящего из одного офиса и имеющего менее 50 персональных компьютеров.

Мы также заметили разницу в эффективности. Мы оценивали способность каждого продукта выявлять как известные, так и неизвестные вирусы, шпионское и рекламное ПО. Продукты блокировали многие вирусы при попытке доступа, что является идеальным поведением, однако, в случае некоторого рекламного программного обеспечения и новых вирусов тестируемые продукты зачастую никак не реагировали до тех пор, пока не начиналась установка вредоносного кода либо его атака. При невозможности обнаружения на основе сигнатуры или шаблона, мы проанализировали возможности каждого продукта по использованию поведенческих технологий для минимизации вреда.

И хотя ни один продукт не был способен упреждающе блокировать каждую угрозу, которую мы предлагали, у каждого продукта были свои собственные, уникальные технологии блокировки или минимизации вреда от этих компьютерных угроз.

ОЦЕНКА УДОБСТВА – сравнение этапов и времени, необходимых на выполнение важных задач

Activity	McAfee Active VirusScan SMB Edition	Sophos Computer Security SBE 2.0	Symantec Client Security 3.1
Установка продукта и внедрение в 10 конечных точках	45 этапов 31 минута	18 этапов 14 минут	104 этапа 33 минуты
Выявление конечных точек с устаревшим защитным ПО	1 этап 4 секунды	0 этапов Мгновенно	4 этапа 9 секунд
Выявление несоответствия конечной точки политике безопасности	Функция отсутствует	0 этапов Мгновенно	Функция отсутствует
Обнаружение незащищенного компьютера	4 этапа 8 секунд	0 этапов Мгновенно	5 этапов 1 минута
Составление отчета (все выявленные случаи обнаружения вредоносного ПО за последние 24 часа на одном компьютере)	6 этапов 31 секунда	6 этапов 28 секунд	10 этапов 48 секунд
Планирование полносистемного сканирования (включая ПНП)	24 этапа 1:22 минуты	6 этапов 17 секунд	15 этапов 35 секунд
Сканирование системы и авторизация одного ПНП для всех конечных точек (исключая время сканирования)	42 этапа 2:10 минут	15 этапов 35 секунд	27 этапов 1:45 минут
Одобрение списка из 3 ПНП для всех конечных точек	19 этапов 1:05 минут	15 этапов 28 секунд	17 этапов 1:20 минут
Защита новой конечной точки	16 этапов 13 минут	9 этапов 5 минут	10 этапов 11 минут
Одобрение исходящего доступа в интернет для приложения	12 этапов 55 секунд	10 этапов 34 секунды	27 этапов 2:32 минуты
Конфигурирование сигнатуры/частоты обновления	6 этапов 45 секунд	3 этапа 11 секунд	10 этапов 30 секунд
Разрешение на исправление приложений в обновлениях	Функция отсутствует	0 этапов Установка по умолчанию	Функция отсутствует

Примечание: этап – это любое движение мышью или нажатие клавиши(клавиш) клавиатуры, которые требуют человеческого решения, например, вход в систему, выбор пункта в меню или подменю, нажатие кнопки, отметка ячейки или расширение меню. Этапы измеряются, начиная с исходного вида на главной странице панели управления каждого продукта.

При тестировании с использованием конфигураций по умолчанию, продукт Sophos применял собственную защиту на основе поведенческого генотипа (Behavioral Genotype Protection) и клиентский брандмауэр (Sophos Client Firewall) для блокирования неизвестных угроз, и делал это более эффективно, чем продукты от McAfee и Symantec. Например, клиентский брандмауэр Sophos Client Firewall успешно заблокировал вирусы на машине, которую мы умышленно заразили, от их дальнейшего распространения по сети. И технология Behavioral Genotype Protection блокировала некоторые исполняемые файлы, как только они были загружены, и до того, как они начали действовать.

Продукт от McAfee успешно обнаружил и удалил настроечные файлы рекламного ПО до того, как они могли быть установлены. Продукт от Symantec успешно действовал против вирусов и их разновидностей, хотя в ходе наших тестов его система поведенческой защиты по умолчанию оказалась неэффективной. Кроме того, нам больше понравилась практика ежедневных обновлений баз данных вредоносного ПО от компаний McAfee и Sophos, в отличие от практики предоставления еженедельных обновлений от компании Symantec, так как своевременное обновление может защитить от абсолютно нового вируса или разновидности старого вируса.

Наш вердикт

После тщательного тестирования продуктов от McAfee, Sophos и Symantec мы пришли к выводу, что Sophos Computer Security SBE 2.0 выделился тем, что явно отвечал интересам малого бизнеса. McAfee Active VirusScan SMB Edition продемонстрировал некоторую эффективность при блокировке, однако его было гораздо труднее устанавливать и управлять им, чем продуктом от Sophos. Продукт Symantec Client Security 3.1 по нашему мнению, по большей части не предназначен для среды малого бизнеса, поскольку у него сложные требования к конфигурации, отсутствует инструментальная панель с выполнимыми опциями, а также продукт показал низкую производительность при сканировании вредоносного ПО.

McAfee Active VirusScan SMB Edition

McAfee Active VirusScan SMB Edition показал смешанные результаты в ходе нашего тестирования. При том, что продукт имеет информативную инструментальную панель и способность блокировать некоторые рекламные программы перед их установкой, его возможности, связанные с функциями брандмауэра, оказались неудобными в работе. Интерфейс управления у McAfee более сложный, чем тот «идеальный» вариант, в котором (по нашему мнению) нуждаются пользователи сферы малого бизнеса. И, к сожалению, процесс установки подвержен ошибкам – вполне вероятно по той причине, что компания McAfee предприняла попытку модифицировать продукт для корпораций вместо того, чтобы заново разработать соответствующий продукт для малого бизнеса.

Начало работы

McAfee Active VirusScan SMB Edition включает продукт McAfee VirusScan Enterprise 8.0i вместе с ProtectionPilot – сервером управления и панелью управления. И при том, что и Sophos, и Symantec интегрируют средства обнаружения шпионского ПО в один продукт, McAfee этого не делает, а предлагает отдельный продукт под названием AntiSpyware Enterprise Module, приобретаемый и устанавливаемый отдельно. Так как мы не можем себе представить, что какая-либо

ОЦЕНКА ПРОИЗВОДИТЕЛЬНОСТИ – сравнение результатов сканирования

Действие (см. прим. 1)	McAfee Active VirusScan SMB Edition	Sophos Computer Security SBE 2.0	Symantec Client Security 3.1
Сканирование по требованию накопителя С: (заражений нет), см. Прим. 2	9:12 минут	5:59 минут	12:34 минуты
Сканирование по требованию накопителя С: (накопитель заражен рекламным ПО)	11:19 минут	10:17 минут	15:11 минут
Сканирование по требованию (одна папка – 5696 файлов, 653 Мб)	2:14 минут	1:54 минуты	3:48 минут
Сканирование по доступу (копия папки – 444 файла, всего 554 Мб)	Выкл.: 2:18 минут Вкл.: 3:16 минут Вновь: 2:51 минута	Выкл.: 2:00 минут Вкл.: 2:18 минут Вновь: 1:59 минут	Выкл.: 2:20 минут Вкл.: 3:07 минут Вновь: 2:28 минут

Примечание 1: Данные результаты являются средним значением по трем измерениям.

Примечание 2: Тест представлен минимальным набором данных, характерным для реальной рабочей станции (накопитель С: содержит примерно 13000 файлов), включая системные файлы Windows. Мы исключили папку с ПО для защиты конечной точки, временную папку Windows, а также процессы сканирования памяти и реестра в целях обеспечения корректности сравнительного анализа.

компания малого бизнеса может обойтись без защиты от шпионского ПО, то предпочли бы, чтобы этот отдельный модуль был интегрирован в основной продукт для устранения лишних шагов по установке и потенциальной путаницы при использовании. В целом установка различных компонентов в составе McAfee Active VirusScan SMB Edition и внедрение этих компонентов в конечных точках заняло больше времени чем, например, установка продукта от Sophos.

Управление и наглядность

После установки администратор может управлять как модулем VirusScan Enterprise, так и модулем AntiSpyware с помощью единой консоли управления ProtectionPilot. Администраторы могут внедрять агентов, управлять конфигурацией политик, устанавливать предупреждения, а также создавать отчеты. Инструментальная панель ProtectionPilot, предоставляющая графический информативный обзор состояния конечных точек и недавно обнаруженных угроз, не предоставляет информацию относительно того, какие именно конечные точки были заражены. Выбирая соответствующие ссылки на инструментальной панели, администраторы могут выполнять такие общие функции как обновление для клиентов, создание отчетов, а также распределение основной политики.

Отчетные функции продукта McAfee достаточны, но им не хватает автоматизации – нет функции оповещения по

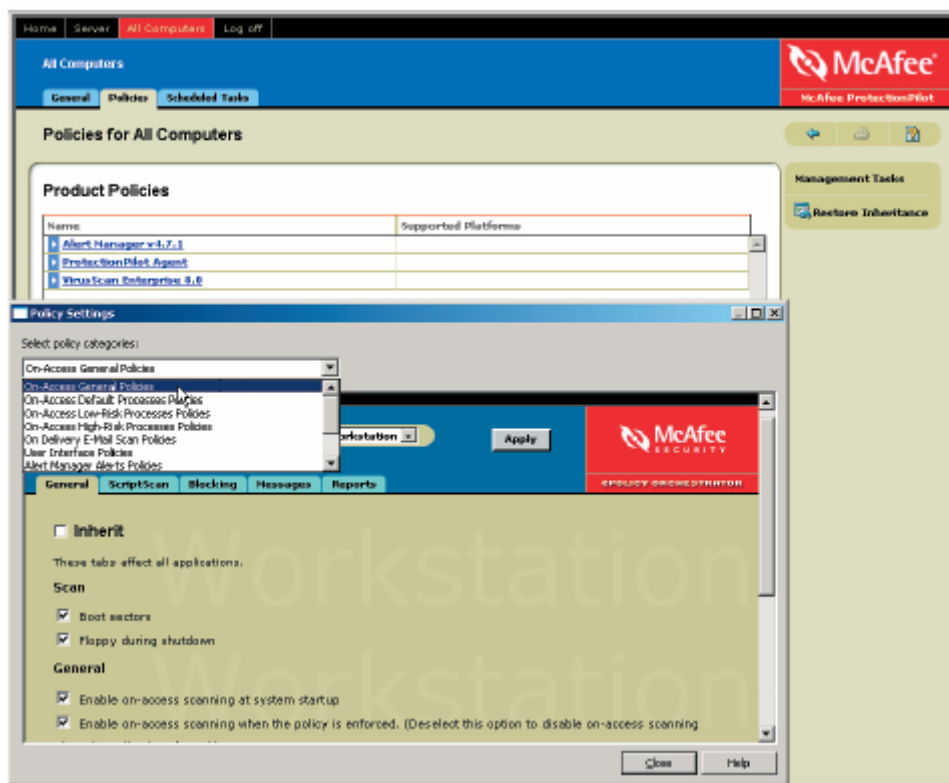
электронной почте третьей стороны (например, ИТ-консультанта) о состоянии безопасности. Отчетность ограничивается созданием скриншотов отчетов (в виде, готовом для печати), которые можно сохранить в виде веб-страницы, веб-архива или текстового файла, а также которые можно вручную приложить к электронному сообщению. Программа

рассылки предупреждений McAfee Alert Manager является отдельным приложением, предоставляющим механизм для рассылки предупреждений или оповещений о текущем состоянии сети посредством электронной почты, пейджера или сообщений локальной сети, однако более продуманные установки по умолчанию и более простая конфигурация сделали бы ее более полезной и удобной для пользования.

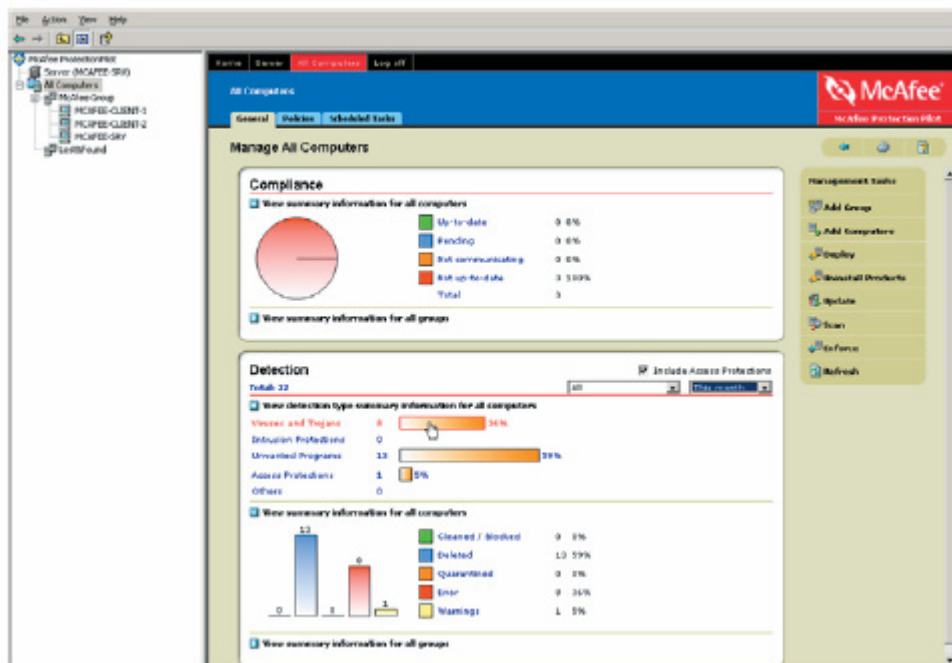
Эффективность

Продукт McAfee оказался эффективным при распознавании, блокировании и удалении более распространенных вирусов, шпионского и рекламного ПО, которые мы применяли в наших тестах. При полносистемном сканировании на компьютере, зараженном целым рядом вирусов, система автоматической очистки от McAfee успешно удалила все, кроме одного приложения; однако, в последнем случае продукт McAfee указал на процедуру очистки, доступную по ссылке на сайте McAfee, которая приводится в тексте подробного описании этого вредоносного ПО, что позволило провести очистку в ручном режиме.

Во время нашего испытания выяснилось, что McAfee особенно успешно



Задания конфигураций McAfee могут перегрузить администраторов малых предприятий, что является неприятной особенностью выбора продукта, исходно ориентированного на корпорации.



Инструментальная панель ProtectionPilot от McAfee включает информативную панель, отражающую состояния соответствия и выявления угрозы.

справилась с обнаружением и удалением установочных файлов рекламного ПО до их установки и перед тем, как данное ПО смогло проникнуть в систему.

Тем не менее, нам показалось, что установки по умолчанию были отчасти агрессивными. Например, при работе с потенциально нежелательными приложениями они удалялись без подсказки. Такое поведение по умолчанию может представлять проблему в случае, если обнаружение стало результатом ошибочного срабатывания либо если подозрительная программа имеет те функции, которые объективно нужны пользователю. Также непросто одобрить конкретное ПНП, так как администратор должен вручную создать исключение для этого на уровне политики группы либо политики конечной точки, но это должно быть сделано обязательно до проведения полного сканирования (которое удалит это ПНП).

При противодействии недавно разработанным вирусам, для которых не было сигнатур, продукт от McAfee оказался не таким успешным. Например, при тестировании недавнего вируса массовой рассылки продукт McAfee позволил вирусу загрузить вредоносный код из интернета, а затем исполнить его, но надо отдать должное продукту от McAfee, так как он все же заблокировал поток элек-

тронных писем с помощью модуля Access Protection, однако сделал он это не так эффективно, как продукт от Sophos, который полностью блокировал попытку загрузки вируса. В случае клавиатурного шпиона, для которого у McAfee не было сигнатуры, модуль Access Protection не смог отразить атаку. В целом мы считаем функцию Access Protection менее эффективной, чем готовый брандмауэр для рабочих станций в вопросе предотвращения повреждений, вызванных вредоносным ПО. Для целей дополнительного уровня защиты продукт от McAfee также включает защиту от переполнения буфера, рассчитанную на конкретные приложения, и данная функция может оказаться полезной для блокировки атак против уязвимостей, которые не исправлены в Internet Explorer и еще приблизительно в 30 различных других приложениях.

В ходе нашего тестирования выяснилось, что в среднем McAfee сервер загружает обновления на ежедневной основе, однако при необходимости имеет возможность загружать обновления более часто. Каждый загруженный файл достаточно объемный, в основном, по 20 МБ, однако обновления от сервера к клиентам меньше по объему. Обновления могут включать и сигнатуры, и обновление ядра, причём они автоматически включаются у клиентов после загрузки, однако

пользователям следует помнить о том, что в отличие от Sophos функция обновления не включает исправления или обновления других частей ПО, кроме относящегося к ядру и сигнатурам; их нужно загружать и устанавливать вручную; поэтому их зачастую игнорируют многие малые предприятия.

McAfee Active VirusScan SMB Edition поддерживает конечные точки, работающие в среде Windows NT или более поздних ОС. Приложение ProtectionPilot не может управлять компьютерами Macintosh, и малые предприятия должны сами приобретать защиту и управлять ею для используемых компьютеров Macintosh. Компания McAfee предлагает защиту от вирусов для серверов электронной почты и интернет-шлюзов в своем продукте McAfee Active VirusScan SMB Edition, равно как и отдельное внешне управляемое решение Total Protection for Small Business.

Вывод

Продукт McAfee Active VirusScan SMB Edition с модулем AntiSpyware Enterprise включает компоненты, необходимые для того, чтобы помочь малым предприятиям защитить свои сети от общих угроз безопасности. Однако, сложная установка, неполная интеграция, а также относительно сложная конфигурация делают его менее чем идеальным выбором.

Цена (5 пользователей, годовая подписка): 369 долл. США (269 долл. + 100 долл. США за AntiSpyware).

Sophos Computer Security Small Business Edition 2.0

Sophos Computer Security SBE 2.0 для малого бизнеса является по нашему мнению, наиболее удобным продуктом из всех, протестированных нами. Это эффективный, хорошо сконструированный и доступный пакет для обеспечения безопасности конечных точек. С помощью несложной установки и удобной (разумной) конфигурации по умолчанию внедрение продукта становится простым и безопасным, а информативная панель инструментов упрощает текущий мониторинг и управление. С точки зрения эффективности в ходе нашего тестирования выяснилось, что продукт Sophos, удачно комбинируя возможности своего

брандмауэра рабочей станции и технологии поведенческого генотипа (Behavioral Genotype Protection), блокирует и отражает неизвестные атаки более эффективно, чем продукты от Symantec и McAfee.

Начало работы

Продукт от Sophos объединяет хорошо интегрированные компоненты с мастером настройки, что снижает шансы на ошибочные действия. Среднестатистический владелец малого предприятия может установить и конфигурировать продукт Sophos для обеспечения эффективной защиты конечных точек в отличие от продуктов McAfee и Symantec, для надлежащей конфигурации которых требуется изрядный технический опыт и терпение. Мы установили и внедрили Sophos Computer Security SBE 2.0 на десять настольных компьютеров и серверов в течение всего 15 минут. В случае продуктов от McAfee и Symantec на это ушло более чем в два раза больше времени, при этом процесс их установки был гораздо больше подвержен ошибкам.

Sophos Computer Security SBE 2.0 включает полный спектр функциональностей: антивирус, антишпионское ПО, брандмауэр для рабочих станций, инструменты отчетности, а также возможности предупреждений. Sophos интегрировала эти компоненты в единый сервер и единую панель управления – Sophos Control Center, который предлагает администраторам понятную и эффективную инструментальную панель, отражающую общее состояние защиты для ПК Windows и Mac, а также и существующие угрозы. Панель инструментов показывает состояние всех управляемых компьютеров, указывая как конечные точки, которые не соответствуют требованиям политик, так и те точки, которые сейчас вообще не управляются – это единственный из тестируемых продуктов, который показывает данную полезную информацию на высшем уровне своего интерфейса.

Управление и наглядность

Панель управления также является входной точкой для выполнения основных задач – от загрузки обновлений и удаления угроз до добавления новых конечных точек в сети, а также конфигурации отчетности и предупреждений. В случае с Sophos мы имели возможность выполнения большинства задач практически всего

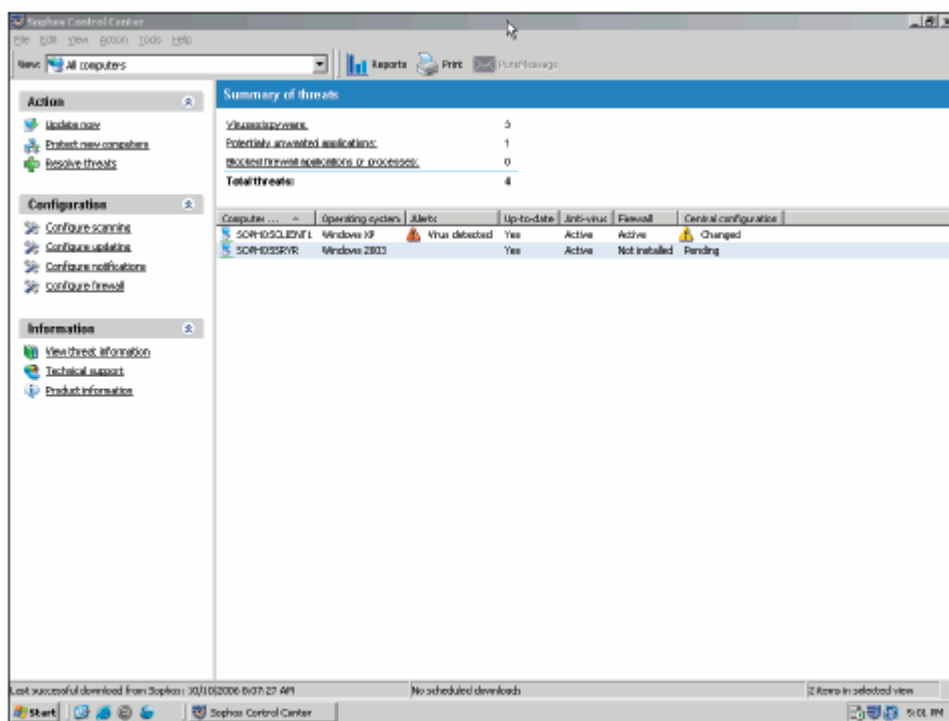
за несколько шагов – управление продуктом может осуществляться даже неопытными пользователями.

Помимо эффективной панели управления Sophos предлагает целый ряд функций, уникальных либо особенно удобных для малого бизнеса. Продукт от Sophos стал единственным, который был способен рассылать еженедельные отчеты об угрозах по электронной почте лицам, находящимся за пределами сети, – это удобный способ для малых предприятий информировать своих ИТ-консультантов о состоянии своих систем безопасности в компании. Sophos также интуитивным образом связывает конфигурации брандмауэров с политиками по потенциально нежелательным приложениям – она предоставляет найденные ПНП и проникновения через брандмауэры так, чтобы администраторы могли лег-

Например, хотя конкретному пользователю можно разрешить использовать конкретное ПНП, это нужно делать на рабочей станции пользователя. Администратор при помощи панели управления может указать, что пользователь уже не соответствует политике по умолчанию, однако, мы бы предпочли, чтобы подобные изменения можно было производить централизованно и внедрять на клиентском компьютере.

Эффективность

В нашем тесте установки безопасности по умолчанию от Sophos обеспечивали защиту от множества различных угроз. Как и другие продукты, Sophos блокировал основные вирусы и разновидности вирусов с помощью комбинации конкретных и общих (generic) сигнатур на основе шаблона. Продукт от Sophos также показал две отличительные осо-

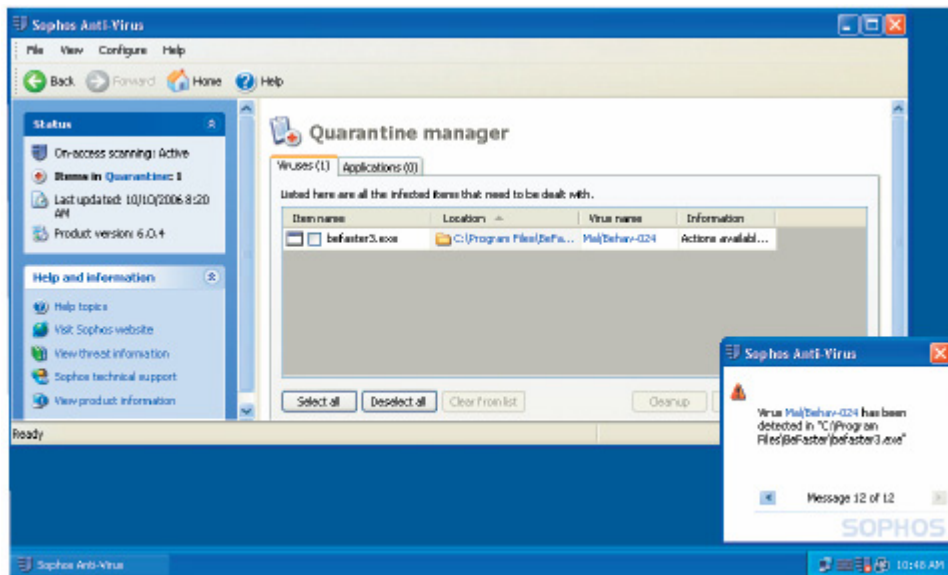


Инструментальная панель Sophos дает обзор высшего уровня и доступ к общим задачам.

ко принимать решения в области политик безопасности, имея под рукой необходимые данные. Так, в частности, полносистемное сканирование выявляет потенциально нежелательные приложения и предоставляет администраторам возможность одобрять все или выборочные ПНП, либо удалять ПНП с помощью функции удаленной очистки.

Sophos, как McAfee и Symantec, также имела трудности с внесением исключений для конкретных пользователей.

бенности, которые доказали свою эффективность в ходе тестирования – защита по поведенческому генотипу (Behavioral Genotype Protection) и клиентский брандмауэр (Sophos Client Firewall), функции, которые обеспечили дополнительную защиту от новых и неизвестных атак вредоносного программного обеспечения. И хотя McAfee и Symantec также используют поведенческие технологии защиты, ни один из этих продуктов в ходе нашего тестирования не показал тот же уровень эффективности.



Защита по поведенческому генотипу от Sophos блокирует рекламное ПО – функция, которая отсутствовала у других продуктов.

В случае двух тестовых экземпляров вредоносного ПО – установочного файла рекламного ПО и клавиатурного шпиона, для которых у Sophos не было сигнатуры, мы заметили, что он применял новую функцию Behavioral Genotype Protection для распознавания подозрительного поведения и блокировки программ до того, как они могли начать исполнение и причинить вред.

После блокировки угрозы интерфейс рекомендовал нам переслать файл в онлайн-центр безопасности Sophos для дальнейшего анализа. Учитывая все возрастающую скорость и распространение атак «нулевого дня», функция Behavioral Genotype Protection предлагает дополнительную и полезную защиту конечных точек.

Компания Sophos также представила наиболее эффективный брандмауэр для рабочей станции в настоящем обзоре. В конфигурации по умолчанию клиентский брандмауэр Sophos успешно блокировал один вирус от дальнейшего распространения по сети с компьютеров, которые мы намеренно заразили. Компонент брандмауэра также включает интерактивные настройки, таким образом, более технически грамотные пользователи могут выбирать опции и позволять или отказывать процессам, которые хотят установить подключения в направлениях «от» или «к» компьютерам сети. И хотя клиентский брандмауэр является важным элементом для ноутбуков, которые выносятся из офиса, наше тестирование показало, что он также эффективен для целей блокировки атак даже на рабо-

чих станциях внутри защищенной сети. Напротив, брандмауэр от Symantec не блокировал эту угрозу в своей конфигурации по умолчанию, а система Access Protection от McAfee, схожая с брандмауэром, оказалась лишь частично эффективной.

Sophos обеспечивает обновление определений вредоносного ПО несколько раз в день, более часто, чем McAfee (ежедневно) и Symantec (еженедельно). В дополнение к обновлениям сигнатур и ядра, предлагаемых всеми поставщиками комплектов ПО, Sophos включает обновления ПО и своих приложений для того, чтобы пользователи малых предприятий могли автоматически получать обновления вместо поиска исправлений или обновлений, которые зачастую не просто найти на сайтах McAfee и Symantec. Мы считаем, что подобные частые и небольшие по объему обновления (менее 250 КБ) полезны для компаний, так как они сужают «окно уязвимости» между обнаружением нового вредоносного ПО и предоставлением защиты. Иногда McAfee выпускает множественные обновления в течение дня. Symantec, как правило, выпускает обновления один раз в неделю (за исключением случаев каких-то эпидемий с вирусами). Как и McAfee, Sophos по умолчанию помогает ноутбукам оставаться «в курсе последних изменений», даже если их владельцы находятся в пути. Хотя конечные точки в первую очередь (по умолчанию) обращаются за обновлениями к своему «родному» серверу в компании, они все же способны получить свои обновления напрямую от

серверов Sophos, если не смогли связаться со своими серверами в компании. И так как обновления в основном очень маленькие, они поступают даже при очень медленном соединении.

Sophos поддерживает более широкий спектр платформ, чем McAfee и Symantec, включая более старые версии операционной среды Windows и Mac OS. Sophos Computer Security SBE 2.0 включает защиту рабочих станций, работающих в Windows 98 или более поздних версиях операционной среды, или Mac OS X и более поздние версии, а также серверов, работающих в Windows Server 2000, 2003 или Small Business Server. Sophos является единственным продуктом, который включает защиту для Macintosh-компьютеров напрямую в панель управления, что становится особенно важным из-за того, что среда Mac OS все чаще становится объектом нападения со стороны вредоносного ПО. McAfee и Symantec работают с компьютерами Macintosh отдельно, с помощью дополнительных продуктов и интерфейса управления, с которыми администраторы должны ознакомиться. Клиентский брандмауэр обеспечивает защиту только на рабочих станциях, работающих в среде Windows 2000 Professional или Windows XP.

Как и продукты от McAfee и Symantec в нашем тесте, Sophos предлагает дополнительные опции для различных вариантов внедрения. Компании, имеющие почтовые серверы Microsoft Exchange, скорее всего предпочтут Sophos Security Suite SBE, при этом те, кому нужен лишь продукт с антивирусной функцией могут выбрать Sophos AntiVirus SBE.

Вывод

Учитывая широкий диапазон действия, легкость в работе и эффективность по блокировке и удалению разных видов вредоносного ПО, пакет Sophos Computer Security SBE 2.0 однозначно является наиболее удобным решением для малого бизнеса по результатам тестов. Он превосходит предложения от компаний McAfee и Symantec по обеспечению безопасности для малого бизнеса.

Цена (5 пользователей, годовая подписка): 269 долл. США.

Symantec Client Security 3.1

Хотя компания Symantec и ориентирует продукт Client Security 3.1 на малый бизнес, на самом деле, он больше подходит для более крупных компаний, где нужно управляться с более сложными задачами, и которые располагают более опытным персоналом для обслуживания этого решения. Мы обнаружили, что продукт более сложно устанавливается и конфигурируется, чем аналогичные решения от McAfee и Sophos; его установки по умолчанию обеспечивали недостаточную защиту от некоторых новых и ранее неизвестных угроз; при этом изменение установок продукта является сложной задачей.

Начало работы

Чтобы заставить работать продукт от Symantec, нужно было изрядно потрудиться. Стандартное внедрение включает множество компонентов – сервер управления, отдельный сервер отчетности, работающий вместе с Microsoft Internet Information Server, две отдельные панели управления – для антивирусного управления и конфигурирования брандмауэра, а также несколько неудобная стартовая конфигурация.

Выполнение минимальной установки и внедрения Symantec с учетом установки исправлений потребовало более 100 этапов, что гораздо более трудоемко, чем при установке продукта от Sophos, самого легкого по установке продукта из всех, протестированных нами. Продукту Symantec Client Security 3.1 не хватает интеграции со службой каталогов Active Directory, поэтому администраторы должны выбирать цели внедрения либо используя сетевой браузер Windows, либо вводя список IP-адресов. Изменение установок почти обязательно требует привлечения персонала техподдержки, поэтому пользователям, не имеющим технической подготовки, следует это учесть. В целом документация очень сложная, поэтому приготовьтесь потратить время на «просеивание» информации о тех различных функциях и возможностях, которые не касаются малого бизнеса.

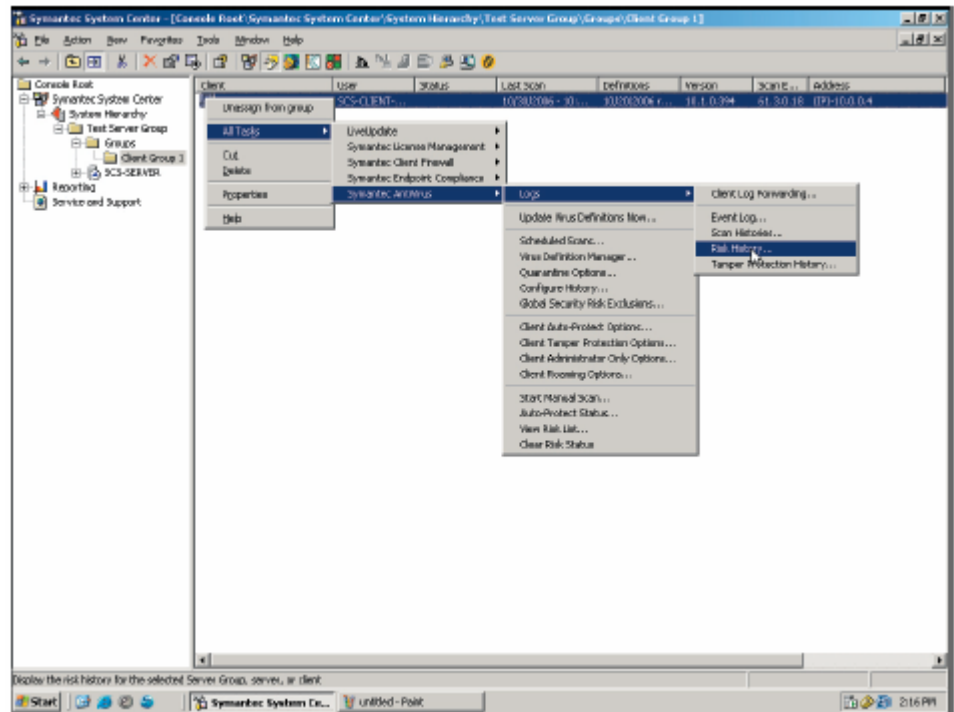
Управление и наглядность

После установки Symantec администраторам приходится иметь дело с различными панелями управления –

это сильно контрастирует с более интегрированным набором инструментов от Sophos и, до некоторой степени, McAfee. Два из наиболее важных интерфейсов включают подключаемую программу MMC (панель управления Microsoft Management Console) для управления антивирусным компонентом и интерфейсом сервера отчетности, а также отдельным, не-MMC приложением для создания файлов политики брандмауэра. Антивирусная

сложность для типичного пользователя из сферы малого бизнеса.

Другие панели управления Symantec включают панель управления карантином, панель хостинга обновлений, а также дополнительную панель предупреждения. Также имеется набор административных инструментов и утилит для создания, просмотра и управления антивирусными политиками и клиентскими внедрениями. Подход Symantec может оказаться



Symantec Client Security 3.1 имеет множество опций; что представляет сложность для пользователей из компаний малого бизнеса.

политика интегрирована в антивирусную панель MMC, однако, так как распространение политики брандмауэра включает прикрепление файлов политики к объектам в антивирусной панели управления, администраторы вынуждены сохранять и организовывать файлы политики брандмауэров напрямую из операционной системы.

Symantec позволяет сосуществовать различным конфигурациям антивируса и брандмауэра в одном домене, разделяя домен на группы серверов для сохранения в них различных индивидуально сконфигурированных объектов. Каждая группа серверов может в свою очередь содержать множественные группы конфигураций для клиентов. И хотя подобная многоуровневая иерархия полезна в среде крупных предприятий, имеющих ряд объектов, она добавляет излишнюю

удручающе сложным для менее подготовленных в техническом плане организаций. Подобная сложность может повлечь неправильную настройку, что в свою очередь может привести к сбоям в области безопасности. В частности, две задачи, которые могут оказаться существенными при определенных условиях, – установка исключений для потенциально нежелательных приложений и изменение стартовой политики брандмауэров – являются наименее интуитивными и наиболее подверженными ошибкам при управлении продуктом Symantec Client Security 3.1.

Продукт от Symantec к тому же включает сложную систему отчетности и предупреждения, хотя ему и не хватает функции автоматической рассылки по электронной почте. Домашняя страница сервера отчетности предоставляет неплохое отражение

состояния угроз, однако, ей не хватает ссылку или кнопок на панели управления, которые имеются в продуктах от McAfee и Sophos.

Эффективность

В нашем тесте продукт от Symantec оказался эффективным в защите от известных вирусов и разновидностей старых вирусов при помощи решений на основе сигнатур и шаблонов, однако, он оказался менее действенным при работе с потенциально нежелательными приложениями. И хотя брандмауэр от Symantec богат функциями, у типичного пользователя из сферы малого бизнеса отсутствуют технические навыки для их надлежащей настройки. Конфигурация брандмауэра по умолчанию не смогла предотвратить загрузку вредоносной программой кода из интернета. Она также не смогла предотвратить превращение зараженной рабочей станции в "зомби", выполняющего массовую рассылку писем. Политику брандмауэра можно сделать более эффективной с помощью ручного добавления ограничений, но это вновь представляется весьма сложной задачей для малого бизнеса, поэтому решение сильно отличается от продукта компании Sophos, имеющего высокий уровень защиты по умолчанию.

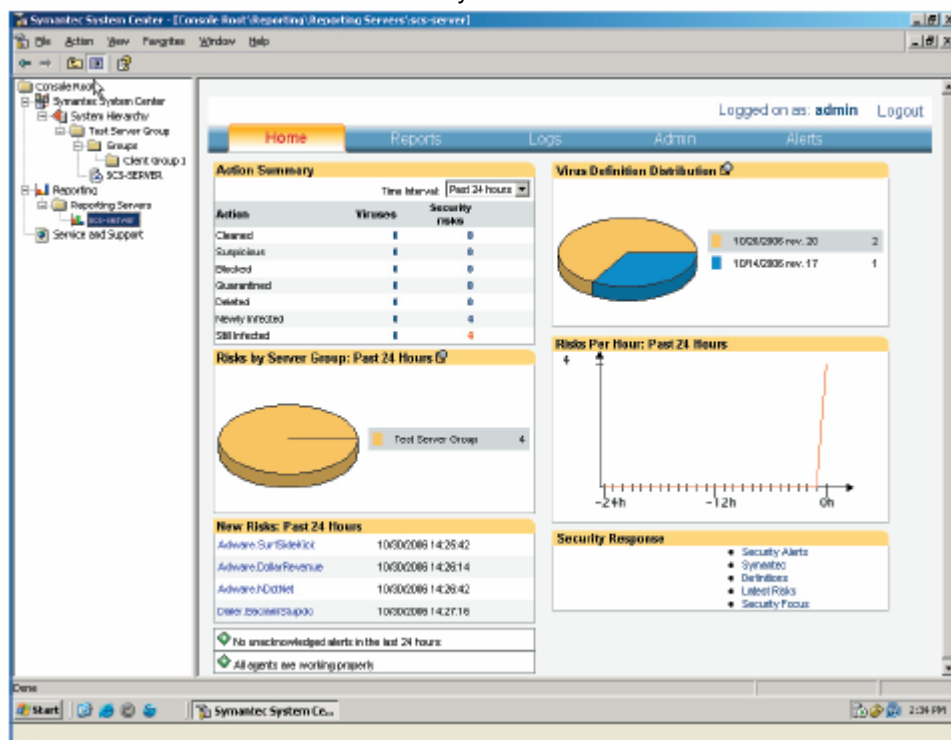
Как и в случае других продуктов, полное сканирование заблокировало использование центрального процессора конечной точки на 100%, что усложняло остальную работу, но, что еще усугубило проблему, у Symantec выполнение такого сканирования заняло больше времени. В наших тестах Symantec выполнял задачи на 50% медленнее, чем Sophos и McAfee.

В рамках наших тестов выяснилось, что Symantec загружал обновления приблизительно один раз в неделю. Каждое обновление занимало примерно 14 МБ. И хотя Symantec иногда выпускает свои обновления чаще, мы предпочли подход компаний Sophos и McAfee, которые выпускают обновления более часто (несколько раз в течение дня или ежедневно).

Symantec Client Security 3.1 поддерживается серверами Windows 2000, Windows XP и Windows 2003. Если необходимо защитить почтовый сервер, можно взять пакет Symantec Client Security и пакет Groupware Protection (групповая защита), а если требуется только антивирусная защи-

та, то есть пакет Symantec AntiVirus в комплекте (или без) с пакетом Groupware Protection. Компания Symantec предлагает пакет антивирусной защиты для пользователей Macintosh, он поставляется и управляется отдельно от продуктов для Windows.

В дополнение к указанному Symantec предлагает комплект интернет-безопасности Norton Internet Security



Домашняя страница сервера отчетности от Symantec предлагает информативное представление информации, но в отличие от панелей управления другими продуктами, у нее нет возможности инициировать действия, связанные с контекстом.

Suite, который может показаться более привлекательным для малых предприятий, но который, однако, является автономным продуктом и не предлагает важных функций, ориентированных на бизнес, таких как возможность управления распространением определений, отчетность, а также выявление и удаленная очистка зараженных систем.

Вывод

Из-за сложности (за исключением случаев наличия компетентного консультанта, имеющего опыт работы с Symantec) мы рекомендуем клиентам сферы малого бизнеса искать другие варианты интегрированного решения по безопасности конечных точек.

Цена (5 пользователей, годовая подписка): 320 долл. США.

Что означает наш рейтинг

Мы установили каждый из этих продуктов в нашу тестовую сеть, настроили их, а затем подвергли 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, брандмау-

эры, и другие средства защиты. Мы также выполнили типичные административные задачи, такие как добавление новых машин в сеть, предоставление исключений отдельным приложениям на индивидуальных ПК, а также изучили действие предупреждений и отчетности. Затем мы оценили работу каждого продукта по шести следующим категориям.

Инсталляция и внедрение. Оценивает 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 конечные точки через службу каталогов Active Directory (которая включена

в Microsoft Small Business Server) или систему Windows NetBIOS.

Удобство и управление. Оценивалась и первичная конфигурация продукта и текущее управление. Мы включили выполнение административных задач, таких как установка конфигурации конечных точек по умолчанию, добавление новой рабочей станции, планирование сканирований, выполнение сканирования по требованию, конфигурация брандмауэра, удаление заражения вредоносным ПО, а также предоставление доступа к потенциально нежелательным приложениям. Мы также включили задачи для конечных пользователей, такие как сканирование файлов, полученных по электронной почте и другими способами, выполнение обновлений для ноутбука в пути, а также применение интерфейса для сбора информации о заблокированных приложениях или файлах. Мы также дали более высокие оценки продуктам с подходящей конфигурацией по умолчанию, что минимизировало затраты на конфигурирование, требуемое для достижения приемлемого уровня защиты.

Наглядность. Включает мониторинг, отчетность, а также возможности формирования предупреждений, которые предлагает продукт. В качестве главного преимущества продукта мы оценивали уровень понятности отображения информации панелью управления по состоянию защищенности клиента, отображение недавних событий, а также деятельность, основанную на задачах.

Эффективность (на основе сигнатур). Оценивает способность продукта блокировать различные виды вредоносного ПО, включая вирусы, разновидности старых вирусов, шпионское и рекламное ПО, а также другие потенциально нежелательные приложения, с помощью конкретных сигнатур или шаблонов. Для обеспечения равных условий мы применяли в тесте экземпляры вредоносного ПО из собственной коллекции, не используя образцы от вендоров.

Эффективность («угрозы нулевого дня»). Оценивает диапазон защиты для остановки или смягчения воздействия от новых или неизвестных вирусов, шпионского ПО и прочих видов

вредоносного программного обеспечения. Мы оценивали антивирусную защиту, защиту от шпионского ПО, брандмауэры настольных систем, защиту от переполнения буфера (buffer overflow), поведенческую защиту по новым вариантам старого кода, а также другие методики поведенческой защиты. 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 вендоров.

Производительность. Оценивает, 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.



Независимая оценка технологической продукции

Контактная информация:

inquiry@cascadialabs.com
www.cascadialabs.com



Этот сравнительный обзор, проведенный независимо компанией Cascadia Labs в октябре и ноябре 2006 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.