Руководство по работе с клиентом Symantec™ Endpoint Protection 14.0.1.x/14.1 для Windows

Symantec

Руководство по работе с клиентом Symantec Endpoint Protection для Windows

Версия продукта: 14.0.1/14.0.1 MP1/14.1

Версия документации: 2

Дата последнего обновления этого документа: декабря 27, 2017

Юридическая информация

воспроизведение, выпуск, публикация Лицензионного программного обеспечения и Документации и разглашение сведений о них правительством США допустимо только при соблюдении условий этого Соглашения.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Техническая поддержка

Техническая поддержка Symantec осуществляется через глобальные центры технической поддержки. Основная функция технической поддержки состоит в том, чтобы отвечать на обращения, связанные с функциями и компонентами продуктов. Группа технической поддержки также отвечает за наполнение электронной базы знаний. Группа технической поддержки работает совместно с другими подразделениями Symantec, чтобы быстро отвечать на запросы клиентов. Например, для обеспечения служб оповещения и обновления описаний вирусов группа технической поддержки работает вместе с группами Product Engineering и Symantec Security Response.

Symantec предлагает следующие варианты поддержки:

- Ряд различных вариантов поддержки, позволяющий подобрать нужные услуги для организации любого размера
- Поддержка по телефону и через Интернет, позволяющая найти решение в кратчайшие сроки и получить самую свежую информацию
- Гарантированное обновление программного обеспечения
- Глобальная поддержка в местное рабочее время или круглосуточно 7 дней в неделю в зависимости от варианта приобретения
- Услуги класса премиум, в том числе Account Management Services

Описание программ поддержки, предлагаемых компанией Symantec, можно найти на веб-сайте компании по следующему URL-адресу:

www.symantec.com/business/support/

Все услуги технической поддержки предоставляются в соответствии с имеющимся соглашением о поддержке и корпоративными политиками поддержки, действительными на момент приобретения.

Обращение в службу технической поддержки

Клиентам с текущим соглашением о поддержке доступна информация службы технической поддержки по следующему URL:

www.symantec.com/business/support/

Перед обращением в службу технической поддержки убедитесь, что система отвечает системным требованиям, приведенным в документации по продукту. Также необходимо находиться в системе, в которой возникла неполадка, на случай если понадобится воспроизвести неполадку.

При обращении в службу технической поддержки укажите следующую информацию:

- Уровень выпуска продукта

- Информация о аппаратном обеспечении
- Доступная память, дисковое пространство и информация о NIC
- Операционная система
- Версия и уровень исправлений
- Топология сети
- Маршрутизатор, шлюз и информация о IP-адресе
- Описание неполадки:
  - Сообщения об ошибках и файлы журналов
  - Действия по устранению неполадок, которые производились перед обращением в Symantec
  - Последние изменения в конфигурации программного обеспечения и изменения сети

Лицензирование и регистрация

Если для продукта Symantec требуется регистрация или ключ лицензии, обратитесь к веб-странице технической поддержки по адресу:

www.symantec.com/business/support/

Служба работы с клиентами

Информация о службе работы с клиентами доступна по адресу:

www.symantec.com/business/support/

Служба работы с клиентами помогает решить нетехнические вопросы, в том числе следующие:

- Вопросы, связанные с лицензированием и сериализацией продукта
- обновления регистрации продукта, например, при изменении имени или адреса;
- общая информация о продукте (функции, доступность языка, местные представители);
- Последняя информация об обновлениях продукта
- информация о гарантиях обновлений и договорах на поддержку;
- Информация о программах покупки продуктов Symantec
- рекомендации по вариантам технической поддержки Symantec;
- нетехнические предпродажные вопросы;
- вопросы, относящиеся к компакт-дискам, DVD-дискам и руководствам.

Ресурсы, касающиеся соглашений о поддержке

Для обращения в Symantec в связи с существующим соглашением о поддержке свяжитесь с региональным представителем службы администрирования соглашений о поддержке:

Азиатско-Тихоокеанский регион и Япония	customercare_apj@symantec.com
Европа, Ближний Восток и Африка	semea@symantec.com
Северная Америка и Латинская Америка	supportsolutions@symantec.com

Оглавление

Глава 1

Начало работы с клиентом Symantec Endpoint Protection

В этой главе рассмотрены следующие вопросы:

- Сведения о клиенте Symantec Endpoint Protection
- Как мне защитить компьютер?
- значки состояния клиента Symantec Endpoint Protection
- Немедленное сканирование клиентского компьютера
- Обновление содержимого клиента с помощью LiveUpdate

Сведения о клиенте Symantec Endpoint Protection

Клиент Symantec Endpoint Protection объединяет в себе несколько уровней обеспечения безопасности, что обеспечивает превентивную защиту компьютера от известных и неизвестных угроз и атак из сети.

Табл. 1-1 описывает каждый уровень защиты.

Табл. 1-1 Типы информации

Уровень	Описание
Защита от вирусов и программ-шпионов	Защита от вирусов и программ-шпионов борется с широким спектром угроз, в том числе с программами-шпионами, червями, троянскими программами, руткитами и программами показа рекламы. Автоматическая защита файловой системы постоянно проверяет все файлы на компьютере на наличие вирусов и угроз безопасности. Автоматическая защита почты в Интернете сканирует входящие и исходящие сообщения электронной почты, передаваемые по протоколам POP3 или SMTP. Функция автоматической защиты Microsoft Outlook сканирует входящие и исходящие сообщения электронной почты Outlook. См. "Управление сканированием на локальном компьютере" на стр. 35.
Превентивная защита от угроз	Технология превентивной защиты включает модуль SONAR, который обеспечивает защиту в реальном времени от атак неизвестного типа. SONAR может остановить атаки раньше, чем традиционные описания на базе сигнатур обнаружат угрозу. Для принятия решений относительно приложений и файлов SONAR использует эвристические данные и анализ репутации файла. См. "Управление SONAR на вашем компьютере" на стр. 81.
Предупреждение последствий использования эксплойтов сети и хоста	Эта защита включает в себя брандмауэр, систему предотвращения вторжений и компонент "Предупреждение последствий использования эксплойтов памяти". ■ Брандмауэр использует в своей работе правила и предотвращает несанкционированный доступ к компьютеру. ■ Система предотвращения вторжений автоматически выявляет и предотвращает атаки из сети. ■ Предупреждение последствий использования эксплойтов памяти блокирует атаки на часто используемые приложения, выполняемые на компьютере Windows. См. "Управление защитой с помощью брандмауэра" на стр. 87. См. "Настройка предотвращения вторжений" на стр. 104. См. "Предотвращение атак на уязвимые приложения" на стр. 106.

Администратор контролирует типы защиты, которые сервер управления загружает на клиентский компьютер. Клиент также загружает на ваш компьютер описания вирусов, определения IPS и обновления продукта. Если вы находитесь в дороге с переносным компьютером, описания вирусов и обновления продукта можно загружать через LiveUpdate.

См. "Обновление содержимого клиента с помощью LiveUpdate" на стр. 20.

Как мне защитить компьютер?

Настройки по умолчанию в клиенте Symantec Endpoint Protection защищают ваш компьютер от многих типов угроз безопасности. Клиент либо автоматически обрабатывает угрозу, либо позволяет вам выбрать способ ее обработки.

Можно проверить, заражен ли компьютер, и выполнить ряд дополнительных задач, если нужно повысить уровень безопасности или быстродействие.

Примечание: В управляемых клиентах некоторые параметры не отображаются, если администратор настроил, чтобы они были недоступны. В неуправляемых клиентах большинство параметров отображаются.

Табл. 1-2 Ответы на часто задаваемые вопросы о защите компьютера

Вопрос	Описание
Как узнать, защищен ли компьютер?	Клиент Symantec Endpoint Protection отображает состояние защиты компьютера. Ваш компьютер лучше всего защищен, когда установлены и обновляются все средства защиты. См. "Как с помощью значков на странице "Состояние" определить, защищен ли клиентский компьютер" на стр. 17. См. "значки состояния клиента Symantec Endpoint Protection" на стр. 16.
Как узнать, заражен ли компьютер?	Если компьютер заражен, могут отображаться какие-либо из указанных ниже сообщений. ■ Обнаружение угроз с помощью сканирования автоматической защиты или сканирования вручную. В этих сообщениях описывается угроза и примененное к ней действие. Для обработки этой угрозы можно выбрать один из нескольких параметров. См. "Реакция на обнаружение вируса или угрозы" на стр. 26. См. "Сведения о результатах сканирования" на стр. 25. См. "Приостановка и откладывание сканирования" на стр. 19. ■ Обнаружение с помощью Download Insight. В этом сообщении отображается информация о вредоносных и непроверенных файлах, обнаруженных функцией Download Insight при попытке их загрузки. См. "Реагирование на сообщения Download Insight с запросом на разрешение или блокирование загружаемого файла" на стр. 28. См. "Типы предупреждений и уведомлений" на стр. 23.

Вопрос	Описание
Как очистить компьютер, если он заражен?	Если появилось окно сканирования, администратор уже задал действие, предпринимаемое компьютером по отношению к заражению. Или вы сможете сами выбрать действие. Если известно, что файл заражен, выберите **Исправить** или **Карантин**. Для плановых сканирований и автоматической защиты в качестве основного действия должно быть задано **Исправить угрозу**, а резервным действием должно быть **Поместить в карантин** или **Удалить**. См. "Реакция на обнаружение вируса или угрозы" на стр. 26. См. "Как работает сканирование на наличие вирусов и программ-шпионов" на стр. 40. См. "Настройка действий при обнаружении вредоносных программ и угроз безопасности" на стр. 66.

Вопрос	Описание
Как повысить уровень защиты компьютера?	По умолчанию управляемый клиентский компьютер имеет максимальный уровень защиты. Администратор может изменить некоторые настройки, чтобы повысить производительность клиента. Если администратор предоставил вам права на изменение настроек защиты вашего компьютера, вы можете выполнять указанные ниже задачи. ■ Запланируйте регулярные полные сканирования, обычно ежедневные или еженедельные. См. "Планирование пользовательских сканирований на клиенте" на стр. 54. ■ Следите за тем, чтобы сканирование на наличие вирусов и программ-шпионов, автоматическая защита, сканирование SONAR, брандмауэр, предотвращение вторжений, предупреждение последствий использования эксплойтов памяти и функция Download Insight всегда были установлены, включены и обновлены. См. "Включение защиты на клиентском компьютере" на стр. 114. См. "Включение автоматической защиты" на стр. 74. См. "Предотвращение атак на уязвимые приложения" на стр. 106. В неуправляемом клиенте вы можете выполнять следующие задачи: ■ Загрузите и установите правильные описания вирусов и содержимое средств безопасности с помощью LiveUpdate. Security Response несколько раз в день выпускает описания вирусов, а кроме того регулярно или по мере необходимости выпускает другое содержимое для обеспечения безопасности. По умолчанию для клиентов Symantec Endpoint Protection запланирован запуск LiveUpdate каждые четыре часа. Кроме того, LiveUpdate можно запустить вручную в любое время. См. "Обновление содержимого клиента с помощью LiveUpdate" на стр. 20. ■ Выполните полное сканирование компьютера так, чтобы были включены все функции повышения эффективности сканирования. По умолчанию полное сканирование выполняется на компьютере еженедельно. Однако вы можете запустить сканирование в любое время. См. "Планирование пользовательских сканирований на клиенте" на стр. 54. См. "Немедленное сканирование клиентского компьютера" на стр. 18.

Вопрос	Описание
Как следует изменить параметры сканирования, если сканирование замедляет мою работу?	Если сканирования замедляют работу компьютера, настройте следующие параметры. ■ Задайте расписание полного сканирования, чтобы оно выполнялось в нерабочее время или когда вы не пользуетесь компьютером. См. "Планирование пользовательских сканирований на клиенте" на стр. 54. ■ Исключите из сканирования приложения и файлы, если вам известно, что они являются безопасными. См. "Исключение объектов из сканирований" на стр. 71. ■ Отключите сканирование сжатых файлов или уменьшите количество уровней развертывания сжатых файлов. См. "Настройка параметров сканирования на наличие вирусов и программ-шпионов" на стр. 63. ■ Выключите параметры повышения эффективности сканирования для сканирований, определенных пользователями. См. "Планирование пользовательских сканирований на клиенте" на стр. 54. **Примечание:** Изменение этих настроек может оказаться невозможным, если они заблокированы администратором.
Что делать, если брандмауэр блокирует просмотр веб-страниц в Интернете?	По умолчанию брандмауэр не блокирует доступ к Интернету. Если вы не можете получить доступ к Интернету, обратитесь к вашему администратору. Ваш администратор мог заблокировать доступ к некоторым веб-сайтам или запретить вашему компьютеру доступ к определенному браузеру. У вас могут быть или отсутствовать права на изменение правил брандмауэра. На неуправляемом клиенте можно изменять правила брандмауэра. Однако не следует изменять или добавлять правило брандмауэра, если вы не знаете, вредоносен или нет трафик, блокируемый правилом брандмауэра. Прежде чем изменять правило брандмауэра, ответьте на следующие вопросы. ■ Является ли легальным веб-приложение, которое осуществляет доступ к Интернету? ■ Являются ли подходящими удаленные порты, доступ к которым осуществляет веб-приложение? Трафик HTTP является законным для веб-приложений. В трафике HTTP используются порты TCP 80 и 443. Трафик через другие порты не следует считать надежным. ■ Является ли IP-адрес веб-сайта, к которому обращается приложение, правильным или допустимым? См. "Добавление правил брандмауэра на клиенте" на стр. 94.

Вопрос	Описание
Какие действия я предпринимаю, когда получаю сообщение в области уведомлений?	Прочтите сообщение в области уведомлений на панели инструментов. Уведомления сообщают об одном из следующих событий. ■ Возможно, компьютер подвергся атаке, и клиент обработал угрозу. См. "Реакция на обнаружение вируса или угрозы" на стр. 26. См. "Реагирование на сообщения с запросом на разрешение или блокирование приложения" на стр. 31. ■ Компьютер автоматически получил новую политику безопасности. Кроме того, в зависимости от типа угрозы можно изучить дополнительную информацию в одном из журналов. См. "Просмотр журналов" на стр. 119.

См. "Проверка типа клиента — управляемый или неуправляемый" на стр. 113.

См. "Управление клиентом" на стр. 108.

значки состояния клиента Symantec Endpoint Protection

Проверьте значок в области уведомлений клиента, чтобы убедиться, что клиент подключен к серверу управления и надлежащим образом защищен. Значок области уведомлений иногда называют значком панели задач.

Значок находится в правом нижнем углу рабочего стола клиентского компьютера. Для отображения часто используемых команд можно также щелкнуть значок правой кнопкой мыши.

Примечание: В управляемых клиентах этот значок не будет показан, если администратор выключил его отображение.

Табл. 1-3 Значки состояния клиента

Значок	Описание
	Клиент работает без ошибок. Он либо работает в автономном режиме, либо не управляется. Неуправляемые клиенты не подключаются к серверу управления.
	Клиент работает без ошибок. Он подключен к серверу и обменивается с ним данными. Для защиты компьютера применяются все компоненты политики безопасности.

Значок	Описание
	На клиенте произошла несущественная ошибка. Например, устарели описания вирусов.
	Клиент не работает, возникла существенная ошибка, истек срок действия лицензии, или по крайней мере одна технология защиты выключена.

См. "Скрытие и отображение значка в области уведомлений на клиенте Symantec Endpoint Protection" на стр. 114.

Как с помощью значков на странице "Состояние" определить, защищен ли клиентский компьютер

В открытом клиенте Symantec Endpoint Protection значки предупреждений в верхней части страницы "Состояние" отражают состояние защиты компьютера. Если в ответ вы должны что-то сделать, рядом со значками находится поясняющий текст.

Табл. 1-4 Значки предупреждений на странице "Состояние"

Значок	Описание
	Показывает, что все типы защиты включены.
	Предупреждает, что описания вирусов или содержимое безопасности на клиентском компьютере устарели. Чтобы получить последние описания вирусов или содержимое безопасности, пользователь может в любой момент запустить LiveUpdate, если это разрешено администратором. Этот состояние может также означать, что требуется перезапуск Symantec Endpoint Protection. На клиентском компьютере Symantec Endpoint Protection, на котором активирована политика целостности хоста, также могут возникать следующие проблемы: ■ Клиентский компьютер не прошел проверку требований к целостности хоста. Для выяснения причины необходимо после проверки просмотреть журнал безопасности функции управления клиентами. ■ Клиентский компьютер не смог загрузить содержимое политики целостности хоста. См. "Обновление содержимого клиента с помощью LiveUpdate" на стр. 20.
	Показывает, что некоторые типы защиты отключены либо срок действия лицензии для клиента истек. Для включения защиты щелкните **Исправить** или **Исправить все**. См. "Включение защиты на клиентском компьютере" на стр. 114.

Немедленное сканирование клиентского компьютера

Просканировать свой компьютер на вирусы и угрозы безопасности можно вручную в любой момент. Сканировать компьютер следует, только если на нем недавно был установлен клиент или появилось подозрение на наличие вируса или угрозы безопасности.

Для сканирования можно выбрать как отдельный файл или устройство USB, так и весь компьютер. Сканирования по запросу включает в себя активное сканирование и полное сканирование. При необходимости можно настроить пользовательское сканирование по запросу.

Можно выполнить немедленное сканирование компьютера одним из следующих способов.

- Как выполнить немедленное сканирование компьютера Windows со страницы "Сканировать"
- Как выполнить немедленное сканирование компьютера Windows со страницы "Состояние"
- Как выполнить немедленное сканирование компьютера из ОС Windows

Как выполнить немедленное сканирование компьютера Windows со страницы "Сканировать"

- На боковой панели клиента выберите **Сканировать**.
  - Чтобы просканировать области, чаще всего подвергающиеся заражению, выберите команду **Запустить активное сканирование**.
  - Чтобы просканировать весь компьютер, выберите команду **Запустить сканирование системы**.
  - Чтобы проверить соответствие политикам безопасности, выберите команду **Сканировать целостность хоста**.

    Примечание: Команда **Сканировать целостность хоста** отображается только в том случае, если для клиента включена политика целостности хоста.

  - В списке сканирований щелкните любое сканирование правой кнопкой мыши и выберите команду **Сканировать сейчас**.

  Сканирование начнется немедленно.

  Можно просматривать ход сканирования, если только администратор не запретил эту опцию. Чтобы просмотреть ход сканирования, щелкните информационную

ссылку, которая появилась для текущего сканирования: **выполняемое *сканирование***.

Дополнительную информацию о параметрах каждого диалогового окна можно получить, щелкнув **Справка**.

Также можно приостановить или отменить сканирование.

Как выполнить немедленное сканирование компьютера Windows со страницы "Состояние"

- В клиенте на странице **Состояние** рядом с пунктом **Защита от вирусов и программ-шпионов** выберите пункт **Параметры > Запустить активное сканирование**.

Как выполнить немедленное сканирование компьютера из ОС Windows

- В окне Windows "Мой компьютер" или "Проводник" щелкните правой кнопкой мыши файл, папку или диск и выберите команду **Проверить на наличие вирусов**.

  Эта функция не поддерживается в 32-разрядных и 64-разрядных операционных системах.

См. "Сведения о результатах сканирования" на стр. 25.

См. "Приостановка и откладывание сканирования" на стр. 19.

См. "Планирование сканирования по запросу или при запуске компьютера" на стр. 57.

См. "Обновление содержимого клиента с помощью LiveUpdate" на стр. 20.

Приостановка и откладывание сканирования

Функция приостановки позволяет остановить сканирование в любой момент, чтобы продолжить его позже. Пользователь может приостановить любое запущенное им сканирование.

Приостанавливать плановые сканирования, настроенные администратором, можно только в случае, если это разрешено администратором. Недоступность кнопки **Приостановить сканирование** означает, что администратор заблокировал функцию приостановки. Если администратор включил функцию откладывания, то пользователь может отложить запланированное администратором сканирование на указанный период времени.

После возобновления сканирование будет продолжено с того же места.

Примечание: Если сканирование приостанавливается в момент проверки сжатого файла, то клиент может выполнить запрос о приостановке с задержкой в несколько минут.

См. "Управление сканированием на локальном компьютере" на стр. 35.

Приостановка сканирования, запущенного пользователем

1. Во время сканирования щелкните **Приостановить сканирование** в окне сканирования.

   Сканирование останавливается, но диалоговое окно сканирования остается открытым до момента повторного запуска.

2. Для продолжения сканирования щелкните **Возобновить сканирование**.

Как отложить запланированное администратором сканирование

1. При выполнении сканирования, запланированного администратором, в окне сканирования выберите **Приостановить сканирование**.
2. В окне **Параметры приостановки сканирования** выполните одно из следующих действий:

   - Для того, чтобы временно приостановить сканирование, выберите **Приостановить**.
   - Для того, чтобы отложить сканирование, выберите **Отложить на 1 час** или **Отложить на 3 часа**.

     Период времени, на который разрешено отложить сканирование, задается администратором. Когда период задержки истекает, сканирование начинает выполняться заново. Число возможных задержек сканирования также задается администратором. При достижении этого числа функция задержки отключается.
   - Для продолжения сканирования без остановки нажмите кнопку **Продолжить**.

Обновление содержимого клиента с помощью LiveUpdate

Чтобы продукты Symantec обеспечивали защиту компьютера от всех новых типов атак, им необходимо регулярно предоставлять свежую информацию. Компания Symantec предоставляет эту информацию с помощью LiveUpdate.

Обновления содержимого — это файлы, предназначенные для обновления продуктов Symantec до самой последней версии. Объем получаемых обновлений содержимого зависит от набора функций защиты, установленного на компьютере. Например, LiveUpdate загружает файлы описаний вирусов для защиты от вирусов и программ-шпионов и файлы описаний IPS для защиты от сетевых угроз.

Начиная с версии 14 у клиентов также есть доступ к полному набору обновлений содержимого в облаке. Сканирования, запущенные на стандартном клиенте, встроенном клиенте или клиенте VDI с подключением к облаку, используют полный набор описаний в облаке.

См. "Как клиенты Windows получают описания из облака" на стр. 51.

LiveUpdate также может по мере необходимости предоставлять усовершенствования для установленного клиента. Эти усовершенствования, как правило, создаются для улучшения совместимости с операционной системой и аппаратным обеспечением, повышения быстродействия или исправления ошибок. Такие обновления могут поступать в управляемые клиенты через управляющий сервер, если он настроен для этого.

LiveUpdate автоматически находит новые файлы содержимого на веб-сайте компании Symantec, а затем заменяет ими старые файлы. Компьютер управляемого клиента обычно получает обновления содержимого со своего управляющего сервера. Управляемые и неуправляемые клиентские компьютеры могут получать это содержимое непосредственно с сервера LiveUpdate. Способ получения обновлений компьютером зависит от того, является он управляемым или неуправляемым, а также от того, как администратор настроил обновления.

Табл. 1-5 Способы обновления содержимого на компьютере

Задача	Описание
Плановое обновление содержимого	По умолчанию функция LiveUpdate запускается автоматически через заданные интервалы. Вы можете также изменить расписание для автоматического запуска LiveUpdate с запланированными интервалами. Запуск LiveUpdate можно запланировать на то время, когда компьютер не используется. В управляемых клиентах можно только настроить LiveUpdate на запуск по расписанию или изменить существующее расписание, если оно включено администратором. Если появляется значок замка, а параметры отображаются серым цветом, вы не можете обновлять содержимое по расписанию или изменять существующее расписание. На неуправляемом клиенте пользователь может отключить или изменить расписание LiveUpdate. См. "Как обновить содержимое по расписанию с помощью LiveUpdate" на стр. 22.
Немедленное обновление содержимого	В зависимости от настройки параметров безопасности LiveUpdate можно запускать немедленно. В следующих ситуациях LiveUpdate требуется запускать вручную: ■ Клиентское ПО установлено недавно. ■ Прошло много времени с момента последнего сканирования. ■ Предполагается наличие вируса или другого вредоносного ПО. **Примечание:** Управляемые клиенты могут запускать LiveUpdate вручную, только когда это разрешено в настроенных администратором параметрах. См. "Как немедленно обновить содержимое с помощью LiveUpdate" на стр. 22.

Как обновить содержимое по расписанию с помощью LiveUpdate

1. На боковой панели клиента нажмите **Изменить параметры**.
2. В разделе **Управление клиентом** нажмите кнопку **Настроить параметры**.
3. В диалоговом окне **Параметры управления клиентами** выберите **LiveUpdate**.
4. На вкладке **LiveUpdate** включите переключатель **Включить автоматическое обновление**.
5. В группе **Частота и время** настройте частоту обновлений.
6. Кроме того, можно включить и настроить параметры рандомизации и обнаружения во время простоя.

   С их помощью можно оптимизировать продолжительность обновления клиента с помощью LiveUpdate.
7. Нажмите кнопку **OK**.

Как немедленно обновить содержимое с помощью LiveUpdate

- На боковой панели клиента выберите **LiveUpdate**.

  Программа LiveUpdate подключается к серверу Symantec, проверяет наличие обновлений, а затем автоматически загружает и устанавливает их.

Глава 2

Реагирование на предупреждения и уведомления

В этой главе рассмотрены следующие вопросы:

- Типы предупреждений и уведомлений
- Сведения о результатах сканирования
- Реакция на обнаружение вируса или угрозы
- Реагирование на сообщения Download Insight с запросом на разрешение или блокирование загружаемого файла
- Реагирование на всплывающие уведомления Symantec Endpoint Protection, отображаемые на компьютерах с Windows 8
- Реагирование на сообщения с запросом на разрешение или блокирование приложения
- Реагирование на сообщения об истечении срока действия лицензии
- Реагирование на сообщения об обновлении ПО клиента

Типы предупреждений и уведомлений

Клиент работает в фоновом режиме, защищая компьютер от вредоносных действий. Иногда клиенту требуется уведомить пользователя о каких-либо действиях или запросить указания.

Табл. 2-1 содержит типы сообщений, которые может увидеть пользователь и на которые требуется реакция.

Табл. 2-1 Типы предупреждений и уведомлений

Предупреждение	Описание
Диалоговое окно "Результаты сканирования"	Если в процессе сканирования будет обнаружен вирус или угроза безопасности, появятся результаты сканирования или диалоговое окно **Результаты обнаружения Symantec Endpoint Protection** со сведениями о заражении. В окне также будет указано действие, которое программа сканирования предприняла по отношению к угрозе. Обычно требуется лишь просмотреть результаты и закрыть окно диалога. Однако при необходимости можно предпринять и дополнительные действия. Если сканирование еще не закончено, в диалоговом окне может отображаться какое-либо сообщение, например ***Имя сканирования*, запущено *Дата* в *Время***. Если сканирование завершено, в диалоговом окне может отображаться какое-либо сообщение, например **Symantec Endpoint Protection - результаты обнаружения**. См. "Сведения о результатах сканирования" на стр. 25.
Другие сообщения	Всплывающие сообщения можно увидеть в следующих ситуациях. ■ Клиент автоматически обновил программное обеспечение. См. "Реагирование на сообщения об обновлении ПО клиента" на стр. 33. ■ Клиент предлагает пользователю разрешить или заблокировать приложение. См. "Реагирование на сообщения с запросом на разрешение или блокирование приложения" на стр. 31. ■ Срок действия пробной лицензии клиента истек. См. "Реагирование на сообщения об истечении срока действия лицензии" на стр. 32.

Предупреждение	Описание

Сообщения значка в области уведомлений	Уведомления возле значка в области уведомлений могут отображаться в следующих ситуациях:
	■ Клиент заблокировал приложение:
	`Traffic has been blocked from this application: Application name`
	Если в клиенте задана блокировка всего трафика, эти уведомления появляются чаще и, как правило, не требуют действий со стороны пользователя. Если клиент разрешает любой трафик, то уведомления появляться не будут.
	См. "Реагирование на сообщения с запросом на разрешение или блокирование приложения" на стр. 31.
	■ Клиент завершил работу приложения:
	`Symantec Endpoint Protection: Атака: обнаружено событие перезаписи структурного обработчика исключений. Symantec Endpoint Protection завершит работу приложения <имя-приложения>`
	См. "Предотвращение атак на уязвимые приложения" на стр. 106.
	■ Клиент обнаруживает атаку из сети на компьютер:
	`Traffic from IP address 192.168.0.3 is blocked from 2/14/2010 15:37:58 to 2/14/2010 15:47:58. Port Scan attack is logged.`
	От пользователя требуется только прочесть сообщения.
	■ Проверка соблюдения требований к безопасности не пройдена. Может блокироваться как входящий, так и исходящий трафик компьютера:
	`Сканирование соответствия не пройдено.`
	См. "Исправление компьютера для прохождения проверки целостности" на стр. 84.

См. "значки состояния клиента Symantec Endpoint Protection" на стр. 16.

Сведения о результатах сканирования

На компьютерах с управляемыми клиентами администратор обычно настраивает запуск полного сканирования не реже, чем раз в неделю. На компьютерах с неуправляемыми клиентами при запуске системы выполняется автоматически созданное активное сканирование. По умолчанию функция автоматической защиты работает на компьютере постоянно.

В процессе сканирования на экране отображается окно с ходом выполнения и результатами сканирования. После завершения сканирования появляется список результатов. Если никакие вирусы и угрозы не были обнаружены, то список останется пустым, а состояние изменится на значение "Выполнено".

Если во время сканирования клиент находит угрозу, то в окне результатов сканирования отображаются результаты, содержащие следующую информацию:

- имена вирусов или угроз безопасности;
- имена зараженных файлов;
- Действия, выполненные клиентом для обработки угроз

Если клиент обнаружит вирус или угрозу, может потребоваться вмешательство пользователя для обработки зараженного файла.

Примечание: Для управляемых клиентов администратор может настроить скрытие окна результатов. Для неуправляемого клиента решение о скрытии или отображении окна принимает пользователь.

Если пользователь или администратор настраивает отображение окна результатов, то с его помощью можно прервать, перезапустить или остановить сканирование.

См. "Сведения об управляемых и неуправляемых клиентах" на стр. 111.

См. "Реакция на обнаружение вируса или угрозы" на стр. 26.

См. "Приостановка и откладывание сканирования" на стр. 19.

Реакция на обнаружение вируса или угрозы

Когда выполняется сканирование, созданное администратором, пользователем или функцией автоматической защиты, может появиться окно результатов сканирования. В этом окне можно немедленно совершить действия над вредоносным файлом. Например, очищенный от вируса файл можно удалить, если у вас есть его копия.

Если приложению Symantec Endpoint Protection необходимо завершить процесс или приложение либо остановить службу, то в окне будет доступна кнопка **Устранить угрозы сейчас**. При наличии угроз, требующих решения пользователя, окно нельзя закрыть.

При необходимости можно отложить выполнение действия над угрозой на более позднее время. Чтобы впоследствии выполнить необходимые действия над файлом, можно использовать карантин, журнал угроз или журнал сканирования указанными ниже способами.

- Откройте журнал угроз, щелкните правой кнопкой мыши на записи об угрозе и выполните необходимое действие.
- Запустите сканирование для повторного обнаружения угрозы. При этом снова появится окно результатов.

Кроме того, можно щелкнуть правой кнопкой мыши на угрозе в диалоговом окне и выбрать действие. Набор доступных действий зависит от того, какие действия были настроены в отношении определенного типа угрозы, обнаруженной во время сканирования.

Реагирование в диалоговом окне результатов сканирования на обнаружение вируса или угрозы

1 В диалоговом окне результатов сканирования выберите файлы, действие с которыми предполагается.

2 Щелкните правой кнопкой мыши выделенный набор и выберите один из следующих вариантов.

Исправить	Удаляет вирус из файла. Этот параметр доступен только для вирусов.
Исключить	Исключить файл из повторного сканирования.
Удалить файл	Удаляет зараженный файл и пытается удалить или исправить все побочные эффекты заражения. Будьте внимательны, выбирая это действие для угроз безопасности. В некоторых случаях удаление угрозы может привести к тому, что приложение перестанет работать.
Отменить действие	Отменяет выполненное действие.
Поместить в карантин	Помещает зараженный файл в карантин. При обработке угроз безопасности клиент также пытается удалить или исправить все побочные эффекты заражения. В некоторых случаях помещение угрозы безопасности в карантин может привести к нарушению функционирования приложения.
Свойства	Показывает информацию о вирусе или угрозе безопасности.

В некоторых случаях действие может быть недоступным.

3 В диалоговом окне нажмите кнопку **Закрыть**.

При наличии угроз, требующих обработки, окно нельзя закрыть. Например, от клиента может потребоваться прерывание процесса или приложения либо остановка службы.

Если пользователю требуется выполнить действие, то будет показано одно из следующих уведомлений:

- **Необходимо устранить угрозу.**
  Появляется в случае, если необходимо завершить процесс. Если пользователь решит удалить угрозу, то снова будет показано окно результатов. Если при этом требуется перезапуск системы, в строке угрозы в этом окне будет показано соответствующее уведомление.

- **Нужно перезапустить систему**
  Появляется в случае, если необходимо выполнить перезапуск.
  Если необходим перезапуск, угроза не будет устранена до тех пор, пока система не будет перезапущена.
- **Удалить угрозу и перезапустить систему**
  Отображается, когда для устранения одной угрозы требуется завершить процесс, а для устранения другой угрозы требуется перезапустить систему.

4 Если открылось диалоговое окно **Устранить угрозы сейчас**, выберите один из следующих вариантов.

- **Устранить угрозы сейчас (рекомендуется)**
  Клиент удалит угрозу. После удаления угрозы может потребоваться перезапуск. В диалоговом окне будет указано, требуется ли перезапуск.
- **Не устранять угрозы**
  Диалоговое окно результатов напоминает, что пользователь по-прежнему должен выполнить действие. Однако окно **Устранить угрозы сейчас** будет скрыто вплоть до перезапуска компьютера.

5 Если диалоговое окно результатов не было закрыто на шаге 3, нажмите кнопку **Закрыть**.

См. "Как функция сканирования реагирует на обнаружение вируса или угрозы" на стр. 49.

См. "Просмотр журналов" на стр. 119.

См. "Управление сканированием на локальном компьютере" на стр. 35.

См. "Управление файлами, помещенными в карантин, на компьютере" на стр. 73.

Реагирование на сообщения Download Insight с запросом на разрешение или блокирование загружаемого файла

В уведомлениях Download Insight отображается информация о вредоносных и неподтвержденных файлах, которые обнаружены функцией Download Insight при попытке их загрузки.

Примечание: Независимо от того, включены уведомления или нет, пользователь получает сообщения, если действие для неподтвержденных файлов имеет значение **Запросить**.

Пользователь или администратор может изменить уровень чувствительности Download Insight к вредоносным файлам. При этом может измениться число получаемых пользователем уведомлений.

Download Insight использует технологию Symantec Insight, которая оценивает и определяет рейтинг файла на основании данных международного сообщества миллионов пользователей.

Уведомление Download Insight показывает следующую информацию об обнаруженном файле.

- Репутация файла
  Репутация файла определяет степень надежности файла. Вредоносные файлы являются ненадежными. Неподтвержденные файлы могут быть как надежными, так и ненадежными.
- Распространенность файла в сообществе
  Распространенность файла является важным фактором. Вероятность наличия угрозы в малоизвестном файле более высока.
- Новизна файла
  Чем новее файл, тем меньше у компании Symantec сведений о нем.

Приведенные сведения помогут принять решение о блокировке или разрешении файла.

Как реагировать на обнаружение Download Insight с запросом на разрешение или блокирование файла при попытке загрузки файла

- В сообщении Download Insight об обнаружении выполните одно из следующих действий.
  - Щелкните **Удалить этот файл с компьютера**.
    Download Insight помещает файл в карантин. Этот параметр отображается только для неподтвержденных файлов.
  - Щелкните **Разрешить этот файл**.
    Может появиться диалоговое окно с запросом, действительно ли вы хотите разрешить этот файл.
    При выборе варианта разрешить неподтвержденный файл, не помещенный в карантин, он автоматически запускается. При выборе варианта разрешить файл, помещенный в карантин, он автоматически не запускается. Этот файл можно запустить из временной папки Интернета.
    Как правило, расположение папки выглядит следующим образом: *диск*:\Users*имя пользователя*\AppData\Local\Microsoft\Windows\Temporary Internet Files, *диск*:\Users*имя пользователя*\AppData\Local\Microsoft\Windows\INetCache или *диск*:\Documents and Settings*имя пользователя*\Local Settings\Temporary Internet Files.

В неуправляемых клиентах при разрешении файла клиент автоматически создает исключение для него на данном компьютере. В управляемых клиентах, если администратор разрешает пользователю создавать исключения, клиент автоматически создает исключение для файла на данном компьютере.

См. "Управление обнаружениями Download Insight на компьютере" на стр. 58.

См. "Принцип принятия решений о файлах с помощью Symantec Insight в Symantec Endpoint Protection" на стр. 50.

См. "Управление сканированием на локальном компьютере" на стр. 35.

Реагирование на всплывающие уведомления Symantec Endpoint Protection, отображаемые на компьютерах с Windows 8

На клиентских компьютерах с Windows 8 всплывающие уведомления об обнаружениях вредоносных программ и о других критических событиях появляются в пользовательском интерфейсе в стиле Windows 8 и на рабочем столе Windows 8. Эти уведомления оповещают пользователя о произошедшем событии либо в пользовательском интерфейсе в стиле Windows 8, либо на рабочем столе Windows 8 независимо от того, какой интерфейс в данный момент просматривает пользователь. Пользователь может просматривать сведения о событии, вызвавшем уведомление, в сообщении на рабочем столе Windows.

Для управляемых клиентов администратор может выключить всплывающие уведомления.

Как реагировать на всплывающие уведомления Symantec Endpoint Protection, отображаемые на компьютерах с Windows 8

1 Во всплывающем уведомлении, отображаемом в верхней части экрана, можно выполнить одну из следующих задач:

- В пользовательском интерфейсе в стиле Windows 8 щелкните уведомление. Появится рабочий стол.
- На рабочем столе щелкните уведомление.

Уведомление исчезнет.

2 Просмотрите результаты обнаружения или другое информационное сообщение, отображаемое на рабочем столе.

В отношении обнаружений вирусов и программ-шпионов, не влияющих на приложения в стиле Windows 8, вам доступно дополнительное действие по исправлению. Если обнаружение влияет на приложения в стиле Windows 8, единственным доступным дополнительным действием является **Исключить**.

Когда вы вернетесь в пользовательский интерфейс в стиле Windows 8, на поврежденном приложении может появиться значок, указывающий на то, что это приложение необходимо загрузить снова.

См. "Управление всплывающими уведомлениями Symantec Endpoint Protection на компьютерах с Windows 8" на стр. 77.

См. "Реакция на обнаружение вируса или угрозы" на стр. 26.

Реагирование на сообщения с запросом на разрешение или блокирование приложения

Когда приложение на компьютере пользователя пытается подключиться к сети, клиентское ПО может предложить пользователю разрешить или заблокировать его. Можно заблокировать приложение, безопасность доступа которого в сеть вызывает сомнения.

Такие уведомления появляются по одной из следующих причин.

- Приложение запросило доступ к сетевому соединению.
- Приложение, работавшее с сетевым соединением, обновилось.
- Администратор обновил программное обеспечение клиента.

При попытке приложения обратиться к сети с локального компьютера может появиться сообщение следующего содержания:

```
IEXPLORE.EXE is attempting to access the network.
Do you want to allow this program to access the network?
```

Реагирование на сообщение с запросом на разрешение или блокирование приложения

1 Если желательно, чтобы при следующей попытке обращения приложения к сети сообщение больше не выводилось, в диалоговом окне выберите **Запомнить ответ и больше не спрашивать об этом приложении**.

2 Выполните одно из следующих действий:

- Для того чтобы разрешить приложению обращение к сети, нажмите **Да**.

- Для того чтобы запретить приложению доступ к сети, нажмите **Нет**.

На неуправляемых и некоторых управляемых компьютерах на странице "Состояние" также можно изменить действие в отношении приложения. Рядом с пунктом "Предупреждение последствий использования эксплойтов сети и хоста" нажмите **Параметры**, а затем нажмите **Показать сетевые операции** или **Показать параметры приложений**.

См. "Разрешение и блокировка приложений, которые уже запущены на клиенте" на стр. 101.

Реагирование на сообщения об истечении срока действия лицензии

Лицензия нужна для обновления описаний вирусов для процессов сканирования и для обновления программного обеспечения. В клиенте можно использовать лицензии двух типов: пробные и оплаченные. Если срок действия пробной лицензии истек, клиент не сможет обновлять содержимое.

Табл. 2-2 Типы лицензий

Тип лицензии	Описание

Пробная лицензия	Если срок действия пробной лицензии истек, в верхней части панели состояния клиента отображается следующее сообщение (красным цветом):
	`Trial License has expired.`
	`Click Details for more information.`
	Если щелкнуть **Сведения**, появится сообщение с датой прекращения загрузки содержимого и просьбой связаться с администратором для приобретения лицензии. На панели состояния также могут отображаться сведения об устаревшем содержимом.
	Кроме того, дату истечения срока действия лицензии можно посмотреть в пользовательском интерфейсе клиента. Для этого выберите команду **Справка > О программе**.

Оплаченная лицензия	Если срок действия оплаченной лицензии истек, сообщение о состоянии лицензии на панели состояния клиента не отображается. Дата истечения срока действия оплаченной лицензии не отображается в разделе **Справка > О программе**. Обновление содержимого (например, описания вирусов и программ-шпионов) будет продолжаться.

При любом типе лицензии следует обратиться к администратору для ее обновления или продления.

См. "Типы предупреждений и уведомлений" на стр. 23.

См. "Просмотр журналов" на стр. 119.

Реагирование на сообщения об обновлении ПО клиента

Если доступно обновление ПО клиента, могут появляться следующие уведомления.

```
Symantec Endpoint Protection has detected that
a newer version of the software is available from
the Symantec Endpoint Protection Manager.
Do you wish to download it now?
```

Обновление ПО клиента также может устанавливаться в фоновом режиме. После завершения установки может появиться сообщение о необходимости перезапуска компьютера.

Как ответить на уведомление об обновлении

1. Выполните одно из следующих действий:
   - Для того чтобы немедленно загрузить программу, нажмите кнопку **Загрузить сейчас**.
   - Если об обновлении необходимо напомнить через некоторое время, нажмите кнопку **Напомнить позже**.
2. Если после начала установки обновленной программы появится сообщение, нажмите **ОК**.
3. При появлении сообщения о завершении обновления следуйте инструкциям на экране, чтобы выполнить перезапуск компьютера. После перезапуска компьютера установка завершается.

Глава 3

Управление сканированием

В этой главе рассмотрены следующие вопросы:

- Управление сканированием на локальном компьютере
- Как работает сканирование на наличие вирусов и программ-шпионов
- Планирование пользовательских сканирований на клиенте
- Планирование сканирования по запросу или при запуске компьютера
- Управление обнаружениями Download Insight на компьютере
- Настройка параметров Download Insight
- Настройка параметров сканирования на наличие вирусов и программ-шпионов
- Настройка действий при обнаружении вредоносных программ и угроз безопасности
- Сведения об исключении объектов из сканирования
- Исключение объектов из сканирований
- Управление файлами, помещенными в карантин, на компьютере
- Включение автоматической защиты
- Включение и отключение раннего запуска защиты от вредоносных программ
- Управление всплывающими уведомлениями Symantec Endpoint Protection на компьютерах с Windows 8
- Основные сведения об отправке данных в Symantec в целях повышения безопасности вашего компьютера

- Применение клиента вместе с центром обеспечения безопасности Windows
- Сведения о SONAR
- Управление SONAR на вашем компьютере
- Изменение настроек SONAR
- Проверка соблюдения требований безопасности с помощью сканирования целостности хоста
- Включение защиты от изменений

Управление сканированием на локальном компьютере

По умолчанию клиент выполняет активное сканирование ежедневно. Индивидуальная настройка сканирования на управляемом клиенте доступна при наличии разрешения администратора. На неуправляемом клиенте в предварительных настройках отключено активное сканирование, но можно управлять собственными сканированиями.

Начиная с версии 14 сканирования имеют доступ к полному набору описаний в облаке.

См. "Как клиенты Windows получают описания из облака" на стр. 51.

Табл. 3-1 Управление сканированием

Задача	Описание
Ознакомьтесь с принципами сканирования	Просмотрите типы сканирований и типы вирусов и угроз безопасности. См. "Как работает сканирование на наличие вирусов и программ-шпионов" на стр. 40.
Обновление описаний вирусов	На компьютере должны быть установлены самые свежие описания вирусов. См. "Обновление содержимого клиента с помощью LiveUpdate" на стр. 20.
Проверьте, включена ли автоматическая защита	Функция автоматической защиты включена по умолчанию. Автоматическая защита всегда должна быть включена. При отключении автоматической защиты также отключается Download Insight, а компонент SONAR не может обнаруживать угрозы эвристически. См. "Включение автоматической защиты" на стр. 74.

Задача	Описание
Просканируйте свой компьютер	Регулярно проверяйте свой компьютер на наличие вирусов и угроз безопасности. Убедитесь, что сканирование выполняется регулярно — для этого следует проверить дату последнего сканирования. См. "Немедленное сканирование клиентского компьютера" на стр. 18. См. "Планирование пользовательских сканирований на клиенте" на стр. 54. В процессе выполнения сканирования на экране можно видеть диалоговое окно с результатами. В этом окне с обнаруженными при сканировании объектами можно выполнить некоторые действия. См. "Реакция на обнаружение вируса или угрозы" на стр. 26. Пользователь может приостановить запущенное им сканирование. На управляемом клиенте администратор определяет, может ли пользователь приостановить запущенное администратором сканирование. См. "Приостановка и откладывание сканирования" на стр. 19. На управляемом клиенте администратор может запустить сканирование Power Eraser с помощью консоли управления. Power Eraser осуществляет тщательное сканирование, которое выявит труднонаходимые угрозы. После завершения сканирования может потребоваться перезагрузка. Администратор вручную выполняет устранение обнаруженных угроз. Средство Power Eraser нельзя запустить прямо из клиента, но оно входит в состав средства поддержки SymDiag. Если загрузить средство SymHelp и запустить сканирование Power Eraser прямо из клиента, журналы не будут отправляться на консоль управления. Не следует локально запускать сканирование Power Eraser с помощью SymHelp, если средство Power Eraser запущено администратором из консоли управления. В противном случае это может негативно повлиять на быстродействие компьютера.

Задача	Описание
Настройте сканирование, чтобы повысить быстродействие компьютера	По умолчанию Symantec Endpoint Protection обеспечивает высокий уровень безопасности при минимальном влиянии на производительность компьютера. Параметры можно настроить, чтобы еще больше повысить производительность компьютера. Для сканирований по расписанию и по запросу можно изменить следующие параметры. ■ Оптимизация сканирования Задайте для оптимизации сканирования значение **Максимальная производительность приложений**. ■ Сжатые файлы Измените число уровней вложения при сканировании сжатых файлов. ■ Возобновляемые сканирования Можно указать максимальное время выполнения сканирования. Сканирование возобновится в период бездействия компьютера. ■ Рандомизированные сканирования Можно указать, что сканирование будет начинаться в случайные моменты времени в пределах заданного интервала. Можно также отключить сканирование при запуске компьютера или изменить расписание плановых сканирований. См. "Настройка параметров сканирования на наличие вирусов и программ-шпионов" на стр. 63. См. "Планирование пользовательских сканирований на клиенте" на стр. 54.

Задача	Описание
Настройте сканирования для повышения уровня защиты компьютера	В большинстве случаев значения параметров сканирования по умолчанию обеспечивают адекватную защиту компьютера. Но в ряде случаев может потребоваться повышение уровня защиты. Повышение уровня защиты может привести к снижению производительности компьютера. Для операций сканирования по расписанию и по запросу можно изменить следующие параметры. ■ Производительность сканирования Задайте для оптимизации сканирования значение **Максимальная производительность сканирования**. ■ Действия при сканировании Измените действия по исправлению, выполняемые при обнаружении вируса ■ Продолжительность сканирования По умолчанию плановое сканирование выполняется до истечения указанного интервала времени и возобновляется, когда клиентский компьютер бездействует. Для продолжительности сканирования можно задать значение **Сканировать до завершения**. ■ Уровень защиты Bloodhound Технология Bloodhound изолирует логические области файлов с целью обнаружения вирусоподобных действий. Для увеличения уровня защиты компьютера можно заменить уровень обнаружения с **Автоматический** на **Агрессивный**. Однако уровень **Агрессивный** чаще вызывает ложные срабатывания. См. "Настройка параметров сканирования на наличие вирусов и программ-шпионов" на стр. 63.
Настройка сканирования для снижения числа ложных срабатываний	Из процесса сканирования можно исключить заведомо безопасный файл или процесс. См. "Исключение объектов из сканирований" на стр. 71.
Отправьте сведения об обнаруженных объектах в Symantec	Клиентский компьютер по умолчанию отправляет информацию об обнаруженных угрозах в Symantec Security Response. Можно отключить отправку целиком или выбрать, какие сведения нужно передать. Компания Symantec рекомендует не отключать отправку. Предоставляемые сведения помогают компании Symantec бороться с новыми угрозами. См. "Основные сведения об отправке данных в Symantec в целях повышения безопасности вашего компьютера" на стр. 77.

Задача	Описание
Управляйте файлами в карантине	Symantec Endpoint Protection помещает зараженные файлы в карантин и перемещает их в расположение, где они не смогут заразить другие файлы компьютера. Если файл, помещенный в карантин, нельзя исправить, то он удаляется. Также можно выполнить с файлом и другие действия. См. "Управление файлами, помещенными в карантин, на компьютере" на стр. 73.

Табл. 3-2 содержит дополнительные настройки сканирования, которые пользователь может изменить, если нужно повысить уровень защиты, увеличить быстродействие или сократить число ложных срабатываний.

Табл. 3-2 Настройки сканирования

Задача	Описание
Измените параметры автоматической защиты, чтобы повысить производительность компьютера или уровень защиты	Можно изменить следующие параметры автоматической защиты. ■ Кэш файлов Убедитесь, что кэш файлов включен (он включен по умолчанию). Если кэш файлов включен, функция автоматической защиты запоминает просканированные чистые файлы и не сканирует их повторно. ■ Параметры сети Когда на удаленных компьютерах включена автоматическая защита, убедитесь, что включен параметр **Только при выполнении файлов**. ■ Можно также указать, что функция автоматической защиты доверяет файлам удаленных компьютеров и использует сетевой кэш. По умолчанию функция автоматической защиты сканирует файлы при записи с локального компьютера на удаленный компьютер. Кроме того, она сканирует файлы, загружаемые на локальный компьютер с удаленных компьютеров. В сетевом кэше хранятся записи о файлах удаленных компьютеров, просканированных функцией автоматической защиты. При наличии сетевого кэша функция автоматической защиты не сканирует один и тот же файл дважды. См. "Настройка параметров сканирования на наличие вирусов и программ-шпионов" на стр. 63.
Управление обнаружениями ELAM	Может потребоваться включить или выключить функцию раннего запуска защиты от вредоносных программ (ELAM) в клиенте, если вы считаете, что она влияет на производительность компьютера. Кроме того, если возникает много ложных срабатываний ELAM, может понадобиться переопределить параметры обнаружения, используемые по умолчанию. См. "Включение и отключение раннего запуска защиты от вредоносных программ" на стр. 76.

Задача	Описание
Управление обнаружением угроз с помощью Download Insight	Download Insight проверяет файлы, которые пользователь пытается загрузить с помощью веб-браузеров, клиентов систем обмена текстовыми сообщениями и других порталов. Download Insight использует информацию из базы данных Symantec Insight, где собираются сведения о репутации файлов. Download Insight на основании рейтинга репутации файла разрешает или блокирует этот файл либо предлагает пользователю предпринять в его отношении действие. См. "Управление обнаружениями Download Insight на компьютере" на стр. 58.
Управление SONAR	Пользователь может настроить параметры SONAR. См. "Управление SONAR на вашем компьютере" на стр. 81.

Как работает сканирование на наличие вирусов и программ-шпионов

Сканирования на наличие вирусов и программ-шпионов обеспечивают выявление и нейтрализацию или удаление вирусов и угроз безопасности на компьютерах. Сканирование устраняет вирус или угрозу следующим образом:

- Модуль сканирования выполняет поиск вирусов, троянских коней, червей и других угроз безопасности в файлах и других компонентах компьютера. У каждой угрозы есть известный шаблон, называемый сигнатурой. Клиент использует файл описаний, в котором содержится набор данных об известных сигнатурах. Модуль сканирования сравнивает все файлы или компоненты с файлом описаний. Если обнаруживается совпадение, файл считается зараженным или подозрительным.
- Модуль сканирования использует файлы описаний, чтобы определить виды угроз. Затем модуль сканирования предпринимает действия по устранению угроз. Модуль сканирования может очистить, удалить или поместить в карантин элемент, который он считает угрозой. Кроме того, модуль сканирования может устранить все побочные эффекты, вызванные угрозой. Предпринимаемые им действия зависят от типа обнаруженной угрозы.
  См. "Как функция сканирования реагирует на обнаружение вируса или угрозы" на стр. 49.
- Начиная с версии 14 на подключенных к облаку стандартных, встроенных клиентах или клиентах VDI в процессе сканирования идет обращение к полному набору описаний в облаке.
  См. "Как клиенты Windows получают описания из облака" на стр. 51.

Примечание: Symantec Endpoint Protection не помещает в карантин и не удаляет угрозу, обнаруженную в приложениях в стиле Windows 8. Вместо этого Symantec Endpoint Protection удаляет угрозу.

В Табл. 3-3 описаны компоненты, которые сканируются клиентом на компьютере.

Табл. 3-3 Компоненты компьютера, которые сканирует клиент

Компонент	Описание
Выбранные файлы	Клиент сканирует отдельные файлы согласно типу сканирования, выбранному вами или запланированному администратором. Кроме того, можно сканировать отдельный файл или папку из Windows. В большинстве типов сканирований необходимые файлы выбираются пользователем.
Память компьютера	Клиент сканирует оперативную память компьютера. Любой программный вирус, вирус загрузочного сектора или макровирус может быть резидентным. Резидентные вирусы копируются в оперативную память компьютера. Вирус может скрытно находиться в памяти до тех пор, пока не произойдет активирующее его событие. Затем вирус может проникнуть на жесткий диск. Если вирус находится в памяти, при сканировании он не будет обезврежен. Однако вирус можно удалить из оперативной памяти, перезагрузив компьютер, когда будет предложено это сделать.
Загрузочный сектор	Клиент проверяет загрузочный сектор компьютера на наличие загрузочных вирусов. Проверяются два следующих элемента: таблицы разделов и главная загрузочная запись.
Съемный носитель	Еще один стандартный способ распространения угроз — через съемные носители, например устройства USB. Когда съемный носитель вставляется в компьютер, клиент не сканирует его автоматически, но можно выполнить сканирование, щелкнув правой кнопкой мыши в среде Windows.

См. "Немедленное сканирование клиентского компьютера" на стр. 18.

Сведения о вирусах и угрозах безопасности

При сканировании Symantec Endpoint Protection выполняет поиск как вирусов, так и угроз безопасности. К угрозам безопасности относятся программы-шпионы, программы показа рекламы, руткиты и другие файлы, которые могут угрожать компьютеру и всей сети.

Кроме того, вирусы и угрозы безопасности могут передаваться по электронной почте и через мгновенные сообщения. Пользователь может по незнанию загрузить угрозу, приняв лицензионное соглашение для другой программы.

Многие вирусы и угрозы безопасности устанавливаются в режиме загрузки без ведома пользователя. Такая загрузка обычно происходит при посещении вредоносных или

зараженных веб-сайтов, и загрузчик приложения устанавливается через разрешенную уязвимость компьютера.

Рис. 3-1 Как вирусы и угрозы безопасности атакуют компьютер

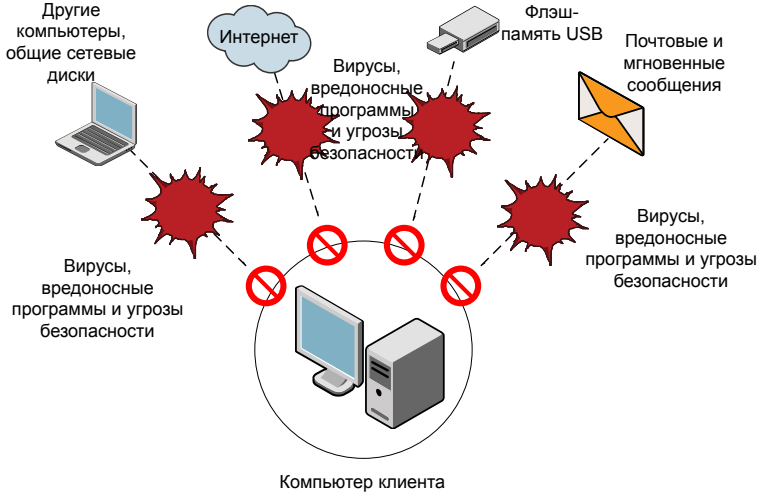

Табл. 3-4содержит перечень типов вирусов и угроз, которые могут атаковать компьютер.

Табл. 3-4 Вирусы и угрозы безопасности

Угроза	Описание
Вирусы	Программы или код, прикрепляющий свою копию к другой компьютерной программе или файлу при их запуске. При запуске зараженной программы вирус активизируется и прикрепляет свои копии к другим программам и файлам. В категорию вирусов входят следующие типы угроз. ■ Вредоносные интернет-боты Программы, выполняющие в Интернете автоматические действия. Боты могут применяться для автоматизации атак на компьютеры или для сбора информации с веб-сайтов. ■ Черви Программы, которые могут размножаться без заражения других программ. Некоторые черви распространяются копированием себя на все доступные диски, а другие размножаются в оперативной памяти, снижая производительность компьютера. ■ Троянские кони Программы, маскирующиеся под полезные приложения, такие как игры или утилиты. ■ Комбинированные угрозы Угрозы смешанного характера, сочетающие применение вирусов, червей, троянских коней и вредоносного кода с попытками воспользоваться известными уязвимостями серверов и Интернета для запуска, передачи и распространения атаки. Такие угрозы используют для быстрого распространения различные методы и техники и могут нанести вред в больших масштабах. ■ Руткиты Программы, скрывающие себя в операционной системе.
Программа показа рекламы	Программы, доставляющие содержимое рекламного характера.
Файлы cookie	Сообщения, отправляемые веб-серверами в веб-браузеры для идентификации компьютера или пользователя.
Программы набора номера	Программы, которые без разрешения и ведома пользователя устанавливают через Интернет телефонную связь с номерами серии 900 или сайтами FTP. Как правило, это делается для взимания платы.
Средства взлома	Программы, используемые хакерами для получения несанкционированного доступа к компьютеру пользователя. Например, такой программой является клавиатурный шпион, отслеживающий и запоминающий все нажатые пользователем клавиши и отправляющий собранные сведения хакеру. Затем хакер может выполнить сканирование портов или поиск уязвимостей. Кроме того, средства взлома могут использоваться для создания вирусов.

Угроза	Описание
Программы-шутки	Программы, которые изменяют или прерывают работу компьютера способом, который их создатель счел смешным или пугающим. Например, такая программа может отодвигать корзину от указателя мыши при попытке удалить элемент.
Программы, вводящие в заблуждение	Приложения, намеренно предоставляющие неверные сведения о состоянии безопасности компьютера. Такие приложения обычно маскируются под уведомления системы безопасности о мнимых заражениях, которые необходимо удалить.
Программы родительского контроля	Программы, отслеживающие или ограничивающие использование компьютера. Программы могут выполняться незаметно и обычно передают данные мониторинга на другой компьютер.
Программа-вымогатель	Категория вредоносных программ, которые блокируют доступ к отдельным документам, но не к самому компьютеру.
Программы удаленного доступа	Программы, которые обеспечивают доступ через Интернет с других компьютеров, что позволяет им собирать информацию либо атаковать или изменять целевой компьютер.
Инструмент оценки безопасности	Программы, используемые для сбора данных и получения несанкционированного доступа к компьютеру.
Программа-шпион	Отдельные программы, которые отслеживают выполняемые в системе действия и отправляют пароли и другую конфиденциальную информацию на другой компьютер.
Следящая программа	Отдельные или дополняющие приложения, которые отслеживают действия пользователя в Интернете и отправляют собранные сведения на компьютер контролера или хакера.

Сведения о конкретных угрозах можно просмотреть на веб-сайте Symantec Security Response http://www.symantec.com/security_response/.

Веб-сайт Symantec Security Response предоставляет последние данные об атаках и угрозах безопасности. Кроме того, здесь можно найти обширную справочную информацию, включая официальные документы и подробное описание вирусов и угроз.

См. "Как функция сканирования реагирует на обнаружение вируса или угрозы" на стр. 49.

О типах сканирований

Symantec Endpoint Protection содержит различные типы сканирования для обеспечения защиты от различных типов вирусов и угроз.

По умолчанию Symantec Endpoint Protection выполняет активное сканирование ежедневно в 12:30. Кроме того, Symantec Endpoint Protection выполняет активное сканирование и при получении новых описаний на клиентском компьютере. На неуправляемых компьютерах Symantec Endpoint Protection предусматривает также сканирование при запуске, которое по умолчанию отключено.

Примечание: Начиная с версии 14 сканирования имеют доступ к полному набору описаний в облаке.

См. "Как клиенты Windows получают описания из облака" на стр. 51.

На неуправляемых клиентах убедитесь, что на компьютере каждый день выполняется активное сканирование. Если возникло подозрение, что на компьютере имеется неактивная угроза, полное сканирование можно запланировать раз в неделю или раз в месяц. При полном сканировании используется большее количество ресурсов компьютера, что может повлиять на его быстродействие.

Табл. 3-5 Типы сканирований

Тип сканирования	Описание
Автоматическая защита	Автоматическая защита постоянно проверяет файлы и электронную почту при их чтении и записи. Эта функция автоматически нейтрализует либо устраняет обнаруженные вирусы и угрозы безопасности. Функция автоматической защиты защищает также некоторые типы исходящей или входящей электронной почты. Начиная с версии 14 на стандартных и встроенных клиентах или клиентах VDI, подключенных к облаку, функция автоматической защиты также использует облачные описания. См. "Сведения о типах автоматической защиты" на стр. 47.
Download Insight	Download Insight увеличивает уровень автоматической защиты благодаря проверке файлов, загружаемых пользователями через браузеры и другие порталы. Download Insight использует информацию из базы данных Symantec Insight, где собираются данные от миллионов пользователей для определения репутации безопасности файлов в сообществе. Download Insight на основании рейтинга репутации файла разрешает или блокирует этот файл либо предлагает пользователю предпринять в его отношении действие. Download Insight функционирует как часть автоматической защиты и требует, чтобы последняя была включена. Если автоматическая защита выключена, то функция Download Insight не работает, даже если она включена. См. "Принцип принятия решений о файлах с помощью Symantec Insight в Symantec Endpoint Protection" на стр. 50.

Тип сканирования	Описание
Сканирования, определенные администратором и пользователем	Для управляемых клиентов администратор может создать плановые сканирования или запускать сканирования по запросу. Для неуправляемых клиентов или управляемых клиентов с разблокированными настройками сканирования можно создавать и выполнять свои собственные сканирования. Сканирования, определенные администратором или пользователем, обнаруживают вирусы и угрозы безопасности, анализируя все файлы и процессы клиентского компьютера. Они также могут проверять память и точки загрузки. Начиная с версии 14 на стандартных и встроенных клиентах или клиентах VDI, подключенных к облаку, эти сканирования используют облачные описания. Доступны следующие типы сканирований, определенные администратором или пользователем. ■ Плановые сканирования Плановые сканирования выполняются на клиентских компьютерах в назначенное время. Сканирования, назначенные на одно время, выполняются последовательно. Если в то время, на которое запланировано сканирование, компьютер окажется выключен, то сканирование выполнено не будет, если не настроена обработка пропущенных сканирований. Запланировать можно активное, полное или выборочное сканирование. Параметры планового сканирования можно сохранить в качестве шаблона. Любое сканирование, сохраненное в качестве шаблона, можно использовать как основу другого сканирования. Шаблоны сканирования позволяют сэкономить время при настройке множества политик. По умолчанию политика содержит шаблон планового сканирования. Плановое сканирование по умолчанию сканирует все файлы и папки. ■ Сканирование при запуске и сканирование по событию Сканирование при запуске выполняется при входе пользователя в систему. Сканирования по событию выполняются при загрузке на компьютер новых описаний вирусов. ■ Сканирования по запросу Сканирования по требованию — это сканирования, запускаемые вручную. Такой вид сканирования можно запустить на странице **Сканировать на наличие угроз**. При обнаружении клиентом большого количества вирусов, программ-шпионов или угроз с высокой степенью риска включается агрессивный режим сканирования. Сканирование перезапускается и использует поиск в Insight. См. "Как работает сканирование на наличие вирусов и программ-шпионов" на стр. 40.
SONAR	SONAR может остановить атаки раньше, чем традиционные описания на базе сигнатур обнаружат угрозу. Для принятия решений относительно приложений и файлов SONAR использует эвристические данные и анализ репутации файла. См. "Сведения о SONAR" на стр. 80.

См. "Управление сканированием на локальном компьютере" на стр. 35.

Сведения о типах автоматической защиты

Компонент автоматической защиты сканирует файлы, а также некоторые типы почтовых сообщений и их вложения.

Автоматическая защита работает только для поддерживаемых клиентов электронной почты. Она не обеспечивает защиту почтовых серверов.

Примечание: Если в открываемом электронном сообщении обнаружен вирус, то открытие сообщения может занять несколько секунд, в течение которых функция автоматической защиты выполняет сканирование.

Табл. 3-6 Типы автоматической защиты

Тип автоматической защиты	Описание
Автоматическая защита файловой системы	Непрерывно сканирует файлы во время их чтения или записи на компьютер. Для файловой системы функция автоматической защиты включена по умолчанию. Она загружается при запуске компьютера. Она проверяет все файлы на наличие вирусов или угроз безопасности и, в случае обнаружения таковых, блокирует их установку. При необходимости она может сканировать файлы с учетом их расширения, файлы удаленных компьютеров, а также дискеты на наличие загрузочных вирусов. Дополнительно она может создавать резервные копии файлов перед попыткой их восстановления, а также завершать процессы и останавливать службы. Функцию автоматической защиты можно настроить для сканирования файлов только с заданными расширениями. В этом случае функция автоматической защиты может определить тип файла, даже если его расширение было изменено вирусом. Функция автоматической защиты сканирует все файлы, даже вложения электронной почты. Даже если не включать автоматическую защиту электронной почты, при включенной функции автоматической защиты файловой системы клиентские компьютеры все равно будут защищены. При запуске вложений электронной почты большинство почтовых программ сохраняют их во временной папке. Функция автоматической защиты сканирует файл в процессе его записи во временную папку и обнаруживает любые вирусы и угрозы безопасности. Вирус будет обнаружен и при попытке пользователя сохранить зараженное вложение на локальном или сетевом диске.

Тип автоматической защиты	Описание
Автоматическая защита интернет-почты	Сканирует входящие сообщения интернет-почты и их вложения на наличие вирусов и угроз безопасности, а также выполняет эвристическое сканирование исходящих сообщений. По умолчанию функция автоматической защиты интернет-почты поддерживает работу с зашифрованными паролями и почтовыми сообщениями, передаваемыми по соединениям POP3 и SMTP. Функция автоматической защиты интернет-почты может работать как в 32-, так и в 64-разрядных системах. Если протокол POP3 или SMTP используется совместно с SSL, клиент распознает безопасные соединения, но не сканирует зашифрованные сообщения. **Примечание:** Из-за возможного снижения быстродействия функция автоматической защиты интернет-почты для POP3 не поддерживается в серверных операционных системах. Сканирование интернет-почты не поддерживает почтовые клиенты на базе протоколов IMAP, AOL или HTTP, такие как Hotmail или Yahoo! Mail.
Автоматическая защита Microsoft Outlook	Загружает вложения входящих сообщений электронной почты Microsoft Outlook и сканирует их на вирусы и угрозы безопасности в процессе чтения сообщения и открытия вложения. Функция автоматической защиты Microsoft Outlook поддерживает версии с Microsoft Outlook 98 по Microsoft Outlook 2016, использующие протокол MAPI или интернет-протокол. Функция автоматической защиты Microsoft Outlook может работать как в 32-, так и в 64-разрядных системах. В процессе установки Symantec Endpoint Protection устанавливает компонент автоматической защиты Microsoft Outlook, если он включен в пакет, а на компьютере уже установлена программа Microsoft Outlook. Загрузка вложений большого объема по медленному соединению может существенно снизить производительность работы электронной почты. При регулярном получении больших вложений эту функцию можно отключить. **Примечание:** Не следует устанавливать компонент автоматической защиты Microsoft Outlook на сервер Microsoft Exchange.
Автоматическая защита Lotus Notes	Сканирует вложения входящей электронной почты Lotus Notes на наличие вирусов и угроз безопасности. Функция автоматической защиты Lotus Notes работает в Lotus Notes 7.x и более поздних версий. В процессе установки Symantec Endpoint Protection устанавливает компонент автоматической защиты Lotus Notes, если он включен в пакет администратором, а на компьютере установлено приложение Lotus Notes.

Как функция сканирования реагирует на обнаружение вируса или угрозы

Действия клиента при обнаружении зараженного файла зависят от типа угрозы. Вначале клиент пытается выполнить первое действие, настроенное для соответствующего типа угрозы, а в случае неудачи — второе действие.

Табл. 3-7 Каким образом функция сканирования реагирует на обнаружение вирусов и угроз безопасности

Тип угрозы	Действие
Вирус	Когда клиент обнаруживает вирус, он по умолчанию предпринимает указанные ниже действия. ■ Сначала клиент пытается удалить вирус из зараженного файла. ■ Если файл удается исправить, то угроза полностью удаляется с компьютера. ■ Если клиенту не удается исправить файл, то он регистрирует ошибку в журнале и перемещает зараженный файл в карантин. См. "Управление файлами, помещенными в карантин, на компьютере" на стр. 73. **Примечание:** Symantec Endpoint Protection не помещает в карантин вирусы, обнаруженные в файлах и приложениях в стиле Windows 8. Вместо этого Symantec Endpoint Protection удаляет такие вирусы.
Угроза безопасности	Когда клиент обнаруживает угрозу безопасности, он по умолчанию предпринимает указанные ниже действия. ■ Клиент помещает зараженный файл в карантин. ■ Клиент пытается удалить или исправить изменения, внесенные этой угрозой. ■ Если клиенту не удается поместить угрозу в карантин, он регистрирует угрозу в журнале и не предпринимает никаких действий с ней. Иногда бывает так, что пользователь устанавливает приложение, содержащее угрозу безопасности, например программу-шпион или программу показа рекламы, о которой он не знает. При обнаружении угрозы безопасности клиент предпринимает указанные ниже действия. ■ Клиент немедленно помещает угрозу в карантин, если это действие не нанесет ущерба компьютеру или не сделает его состояние нестабильным. ■ В противном случае перед тем, как поместить угрозу в карантин, клиент ждет окончания процесса установки приложения, а затем исправляет побочные эффекты угрозы. **Примечание:** Symantec Endpoint Protection не помещает в карантин угрозы безопасности, обнаруженные в файлах и приложениях в стиле Windows 8. Вместо этого Symantec Endpoint Protection удаляет угрозу.

Параметры обработки вирусов и угроз безопасности можно независимо настроить для каждого типа сканирования. Действия можно настраивать на уровне категории угроз или отдельной угрозы.

Принцип принятия решений о файлах с помощью Symantec Insight в Symantec Endpoint Protection

Компания Symantec собирает сведения о файлах с помощью своего глобального сообщества, состоящего из миллионов пользователей, и своей сети Global Intelligence Network. Собранная информация доступна в облаке для всех продуктов Symantec посредством базы данных Symantec Insight. Symantec Insight содержит данные о репутации файлов и последние описания вирусов и программ-шпионов.

Продукты Symantec используют данные Insight для защиты клиентских компьютеров от новых, целенаправленных и меняющихся угроз. Иногда эти данные называются облачными, поскольку они находятся не на клиентском компьютере. Для получения информации Symantec Endpoint Protection отправляет запросы в Insight. Эти запросы еще называются поиском данных репутации, поиском в облаке или поиском в Insight.

Рейтинги репутации в Insight

Symantec Insight определяет уровень угрозы каждого файла — так называемый рейтинг безопасности. Рейтинг известен и как репутация файла.

Insight определяет рейтинг безопасности, проверяя следующие характеристики файла и его контекста.

- Источник файла
- Новизна файла
- Распространенность файла в сообществе
- Другие показатели безопасности, например связь файла с вредоносным ПО.

Insight Lookup

Компоненты сканирования в Symantec Endpoint Protection используют Insight для принятия решений в отношении файлов и приложений. Защита от вирусов и программ-шпионов включает компонент под названием Download Insight. Для принятия решений в отношении файлов Download Insight необходима информация о репутации. SONAR также использует данные о репутации в своей работе.

Параметры Insight Lookup можно изменить. Выберите **Изменить параметры > Управление клиентом > Отправка**.

Начиная с версии 14 на стандартных клиентах и встроенных клиентах или клиентах VDI поддерживается поиск информации о репутации в Insight и поиск описаний в облаке для

автоматической защиты, плановых сканирований и сканирований вручную. Symantec рекомендует не отключать этот параметр.

Предупреждение! Для обнаружения угроз средства Download Insight, SONAR, а также сканирования на наличие вирусов и программ-шпионов используют поиск в Insight. Symantec рекомендует разрешить запросы Insight на постоянной основе. Отключение запросов приводит к отключению функции Download Insight и может снизить эффективность эвристического анализа SONAR и сканирований на наличие вирусов и программ-шпионов.

Отправка сведений по репутации файла

По умолчанию клиентский компьютер отправляет в Symantec Security Response для анализа информацию об обнаружениях на основе репутации. Эта информация позволяет обновить базу данных репутаций Insight и последние описания в облаке. Чем больше клиентов отправляют информацию, тем более полезной становится база данных репутации.

Компания Symantec рекомендует включить отправку сведений для задач обнаружения репутации.

См. "Управление обнаружениями Download Insight на компьютере" на стр. 58.

См. "Основные сведения об отправке данных в Symantec в целях повышения безопасности вашего компьютера" на стр. 77.

Как клиенты Windows получают описания из облака

Начиная с версии 14 стандартные и встроенные клиенты или клиенты VDI в Symantec Endpoint Protection обеспечивают защиту в реальном времени с использованием облачных описаний. В предыдущих версиях были доступны отдельные функции защиты, работающие в облаке, например Download Insight. Теперь все функции защиты от вирусов и программ-шпионов используют описания в облаке для оценки файлов. Содержимое в облаке включает в себя полный набор описаний вирусов и программ-шпионов, а также последнюю информацию о файлах и потенциальных угрозах, известную Symantec.

Клиенты поддерживают содержимое в облаке.

Облачное содержимое включает уменьшенный набор описаний, который обеспечивает полную защиту. Когда клиенту требуются новые описания, он загружает их или ищет в облаке для повышения производительности и скорости.

Тип вашего клиента должен поддерживать содержимое в облаке.

Тип клиента можно проверить в меню **Справка > Устранение неполадок > Параметры установки**.

Начиная с версии 14 и стандартный клиент, и встроенный клиент или клиент VDI поддерживают содержимое в облаке.

Все сканирования автоматически используют облачные запросы.

Облачные запросы получают информацию о репутации файлов из базы данных Symantec Insight и проверяют описания в облаке.

- Плановые сканирования и сканирования по требованию автоматически используют облачные запросы.
- Функция автоматической защиты также автоматически выполняет поиск в облаке. Теперь автоматическая защита работает в режиме пользователя, а не в режиме ядра в целях сокращения использования памяти и повышения быстродействия.

Помимо уменьшения размера занимаемой памяти, служба Intelligent Threat Cloud позволяет на 15 % сократить продолжительность сканирования.

Клиенты автоматически отправляют запросы информации о репутации файлов в Symantec.

Что такое файлы портала?

Download Insight отмечает файл как файл портала во время проверки файлов, загруженных из поддерживаемого портала. Для оценки репутации файлов портала при плановом сканировании, сканировании по требованию, а также в функциях автоматической защиты и Download Insight применяется уровень чувствительности, заданный для Download Insight.

Примечание: Компонент Download Insight должен быть включен, чтобы файлы были отмечены как файлы портала.

Поддерживаемые порталы: Internet Explorer, Firefox, Microsoft Outlook, Outlook Express, Google Chrome, Windows Live Messenger и Yahoo Messenger. Список порталов (или список порталов автоматической защиты) относится к содержимому защиты от вирусов и программ-шпионов, загружаемого LiveUpdate на сервер управления или клиент.

Для оценки внешних файлов сканирования и Download Insight всегда используют внутренний уровень чувствительности по умолчанию, заданный Symantec. Этот уровень позволяет обнаруживать только самые опасные файлы.

Пример использования облачных запросов

Для иллюстрации принципа работы службы Intelligent Threat Cloud для защиты клиентов можно привести следующий пример.

- Вы пытаетесь загрузить файл с помощью Internet Explorer. Download Insight проверяет безопасность файла, используя собственный уровень чувствительности и сведения о репутации из базы данных Symantec Insight в облаке.
- Download Insight убеждается в безопасности файла, разрешает его загрузку и отмечает файл как файл портала.
- Позднее Symantec накапливает еще больше информации о файле из сети Global Intelligence Network. Symantec отмечает файл как потенциально опасный и обновляет сведения в базе данных о репутации. Symantec может добавить обновленную сигнатуру файла к облачным описаниям.
- Если вы откроете файл или запустите сканирование, функция автоматической защиты или сканирование получат актуальную информацию о файле из облака. Теперь файл будет считаться потенциально опасным.

Обязательные и рекомендуемые параметры

По умолчанию Symantec Endpoint Protection использует облако. При отключении любого из указанных параметров возможности защиты в облаке будут ограничены.

- Автоматическая защита
  Автоматическая защита должна быть включена. Функция автоматической защиты включена по умолчанию.
- Download Insight
  Чтобы в будущем загружаемые файлы отмечались как файлы портала, должен быть включен компонент Download Insight. Если Download Insight отключен, все загружаемые файлы обрабатываются как внешние. Сканирования обнаруживают только самые опасные внешние файлы.
  См. "Управление обнаружениями Download Insight на компьютере" на стр. 58.
- Insight Lookup
  Функция Insight Lookup должна быть включена. Insight Lookup управляет поиском информации о репутации и описаний в облаке. По умолчанию этот компонент включен.

  Предупреждение! Если Insight Lookup отключен, защита в облаке не работает.

- Отправка
  Symantec рекомендует разрешить отправку информации в Symantec. Данные, передаваемые в Symantec, помогают повысить эффективность обнаружения. Информация о потенциальных вредоносных программах, способных атаковать компьютеры, позволяет повысить информированность об угрозах безопасности и скорость их устранения. Symantec делает все возможное для предотвращения распространения личной информации при передаче анонимных данных.

См. "Основные сведения об отправке данных в Symantec в целях повышения безопасности вашего компьютера" на стр. 77.

Планирование пользовательских сканирований на клиенте

Плановые сканирования на клиенте Symantec Endpoint Protection — это важный компонент защиты от угроз безопасности. Для того чтобы компьютер был надежно защищен от вирусов и угроз безопасности, плановое сканирование должно выполняться не реже раза в неделю. Созданные сканирования отображаются в окне **Сканирование на наличие угроз**.

Примечание: Если плановое сканирование было создано администратором, то оно будет показано в списке сканирований в панели **Просканировать на наличие угроз**.

Для выполнения планового сканирования компьютер должен быть включен, а службы Symantec Endpoint Protection — загружены. По умолчанию службы Symantec Endpoint Protection загружаются вместе с системой.

Для управляемых клиентов администратор может переопределить эти параметры.

См. "Немедленное сканирование клиентского компьютера" на стр. 18.

См. "Управление сканированием на локальном компьютере" на стр. 35.

При настройке планового сканирования учитывайте следующие важные моменты:

Для пользовательских сканирований не требуется, чтобы пользователь находился в системе.	Если пользователь, который настроил сканирование, не вошел в систему, Symantec Endpoint Protection все равно выполнит сканирование. Можно указать, что клиент не должен выполнять сканирование, если пользователь вышел из системы.
Несколько одновременных сканирований запускаются поочередно	Если на одно и то же время запланировано несколько сканирований, то сканирования выполняются последовательно. После завершения одного сканирования начинает выполняться другой. Например, на компьютере можно запланировать три сканирования на 1:00 ночи для проверки разных дисков. Первое сканирование проверяет диск C, второе сканирование проверяет диск D, а третье сканирование проверяет диск E. В таком случае лучше всего создать одно плановое сканирование, проверяющее диски C, D и E.

Пропущенные плановые сканирования могут не выполниться.	Если компьютер по какой-то причине пропускает запланированное сканирование, по умолчанию Symantec Endpoint Protection пытается повторить сканирование, пока оно не запустится или пока не истечет определенный промежуток времени. Если Symantec Endpoint Protection не может запустить пропущенное сканирование в пределах интервала повтора, сканирование не выполняется.
Время запланированного сканирования может варьироваться	Symantec Endpoint Protection может не использовать запланированное время, если последнее сканирование было выполнено в другое время из-за настроек продолжительности сканирования или пропущенного планового сканирования. Например, можно настроить запуск еженедельного сканирования на каждое воскресенье в полночь, с интервалом повтора в один день. Если компьютер пропустит сканирование и запустится в 6 часов утра понедельника, сканирование выполнится в 6 часов утра. Следующее сканирование выполняется через неделю в понедельник в 6:00, а не в воскресенье в полночь. Если компьютер не запускался до 6:00 четверга, что на два дня превышает установленный интервал повтора, Symantec Endpoint Protection не повторяет попытку сканирования. Для повторения попытки сканирования он ожидает полуночи следующего воскресенья. В любом случае при рандомизировании времени запуска сканирования можно изменить время последнего выполнения сканирования.

Также можно создать сканирование по запросу или сканирование при запуске.

См. "Планирование сканирования по запросу или при запуске компьютера" на стр. 57.

Как задать расписание пользовательского сканирования

1. На боковой панели клиента щелкните **Проверить на наличие угроз**.
2. Выберите **Создать сканирование**.

3 В окне **Создать новое сканирование - Что следует сканировать** выберите один из следующих типов плановых сканирований:

Активное сканирование	Проверяет области компьютера, которые наиболее часто подвергаются заражению вирусами и угрозами. Активное сканирование нужно выполнять каждый день.
Полное сканирование	Проверяет весь компьютер на наличие вирусов и угроз безопасности. Полное сканирование можно выполнять раз в неделю или раз в месяц. Полное сканирование может привести к снижению производительности компьютера.
Выборочное сканирование	Проверяет отдельные области компьютера на наличие вирусов и угроз безопасности.

4 Нажмите кнопку **Далее**.

5 Если был выбран вариант **Выборочное сканирование**, укажите объекты сканирования, включив соответствующие переключатели, а затем нажмите кнопку **Далее**.

Ниже приведено описание значков.

Файл, диск или папка не выбраны. Если элементом является диск или папка, входящие в них папки и файлы также не выбраны.

Выбран отдельный файл или папка.

Выбран отдельный диск или папка. Выбраны все вложенные элементы папки или диска.

Папка или диск не выбраны, но выбраны один или несколько вложенных элементов.

6 В диалоговом окне **Создать сканирование - Параметры сканирования** можно изменить следующие параметры.

Типы файлов	Укажите расширения для файлов, которые должен сканировать клиент. По умолчанию сканируются все файлы.
Действия	Измените первое и второе действия, которые должны выполняться при обнаружении вирусов и угроз безопасности.
Уведомления	Введите сообщение, которое должно появляться при обнаружении вируса или угрозы безопасности. Кроме того, можно включить или выключить отправку уведомления перед исправлением.
Дополнительные параметры	Настройте дополнительные параметры сканирования, в частности, отображение диалогового окна результатов.
Повышение эффективности сканирования	Укажите, какие компоненты компьютера должен сканировать клиент. Набор вариантов зависит от значения, выбранного на шаге 3.

7 Нажмите кнопку **Далее**.

8 В окне **Создать сканирование - Когда выполнять сканирование** выберите пункт **В указанное время**, затем нажмите кнопку **Далее**.

9 В диалоговом окне **Создать сканирование - Расписание** в разделе **Расписание сканирования** укажите периодичность и время сканирования, затем нажмите кнопку **Далее**.

10 В разделе **Продолжительность сканирования** можно указать время, в течение которого должно быть завершено сканирование. Время запуска сканирования можно рандомизировать.

11 В разделе **Пропущенные плановые сканирования** можно указать интервал, в течение которого можно повторить попытку сканирования.

12 В диалоговом окне **Создать сканирование - Имя сканирования** введите имя и описание для созданного сканирования.

Например, сканирование можно назвать "Утро пятницы"

13 Нажмите кнопку **Готово**.

Планирование сканирования по запросу или при запуске компьютера

Пользователь может дополнить плановые сканирования автоматическими сканированиями при включении компьютера или входе в систему. Часто сканирования

при запуске ограничиваются наиболее важными папками, такими как папка Windows и папки с шаблонами Microsoft Word и Microsoft Excel.

При периодическом сканировании одного и того же набора файлов и папок рекомендуется создать сканирование по запросу, в котором будут перечислены сканируемые элементы. Этот позволяет в любой момент быстро проверить заданный набор файлов и папок на наличие вирусов и угроз безопасности. Сканирования по запросу запускаются вручную.

Если существует несколько сканирований при запуске, они будут выполняться последовательно в порядке создания. Администратор может запретить пользователю настройку клиента, тогда создание сканирований при запуске будет невозможным.

См. "Немедленное сканирование клиентского компьютера" на стр. 18.

Планирование сканирования по запросу или при запуске компьютера

1. На боковой панели клиента щелкните **Проверить на наличие угроз**.
2. Выберите **Создать сканирование**.
3. Укажите объекты и параметры планового сканирования.

   См. "Планирование пользовательских сканирований на клиенте" на стр. 54.
4. В диалоговом окне **Создать новое сканирование - Когда выполнять сканирование** выполните одно из следующих действий.
   - Щелкните **При запуске**.
   - Щелкните **По запросу**.
5. Нажмите кнопку **Далее**.
6. В диалоговом окне **Создать сканирование - Имя сканирования** введите имя и описание для созданного сканирования.

   Например, сканирование можно назвать "Мое сканирование 1"
7. Нажмите кнопку **Готово**.

Управление обнаружениями Download Insight на компьютере

Автоматическая защита содержит компонент Download Insight, который проверяет файлы, которые вы пытаетесь загрузить через веб-браузеры, клиенты текстовых сообщений или другие порталы. Чтобы компонент Download Insight работал, должна быть включена автоматическая защита.

Поддерживаемые порталы: Internet Explorer, Firefox, Microsoft Outlook, Outlook Express, Windows Live Messenger и Yahoo Messenger.

Примечание: В журнале угроз для обнаружения Download Insight отображаются сведения об угрозе только для первого приложения портала, сделавшего попытку загрузки. Например, пользователь пытался с помощью Internet Explorer загрузить файл, который определяется компонентом Download Insight как вредоносный. Если затем он попробует загрузить его с помощью Firefox, в поле **Загружено** сведений об угрозе в качестве портала будет отображаться Internet Explorer.

Примечание: Функция автоматической защиты может также сканировать файлы, полученные пользователями в виде вложений электронной почты.

Табл. 3-8 Управление обнаружениями Download Insight на компьютере

Задача	Описание
Сведения о том, как Download Insight использует информацию о репутации для принятия решений в отношении файлов	Download Insight определяет, что загруженный файл может представлять угрозу, на основании сведений о репутации файла. Для принятие решений в отношении загруженных файлов Download Insight использует только информацию о репутации. При принятии решений он не использует сигнатуры или эвристики. Если Download Insight разрешает файл, то затем система автоматической защиты или SONAR сканирует файл, когда пользователь открывает или выполняет его. См. "Принцип принятия решений о файлах с помощью Symantec Insight в Symantec Endpoint Protection" на стр. 50.
Убедитесь, что запросы Insight включены.	Для принятие решений в отношении файлов Download Insight необходима информация о репутации. Если отключить запросы Insight, компонент Download Insight будет работать, но не может обнаруживать угрозы. Запросы Insight включены по умолчанию. См. "Основные сведения об отправке данных в Symantec в целях повышения безопасности вашего компьютера" на стр. 77.
Как реагировать на обнаружения Download Insight	Когда Download Insight обнаруживает угрозу, может появиться уведомление. Для управляемых клиентов администратор может выключить уведомления об обнаружениях Download Insight. Если уведомления включены, при обнаружении Download Insight вредоносных или неподтвержденных файлов будут выдаваться сообщения. Неподтвержденные файлы пользователь должен разрешить или блокировать. См. "Реагирование на сообщения Download Insight с запросом на разрешение или блокирование загружаемого файла" на стр. 28.

Задача	Описание
Создание исключений для конкретных файлов или веб-доменов	Вы можете создать исключение для приложения, которое вы загружаете. Можно создать исключение для конкретного веб-домена, если известно, что он надежный. По умолчанию Download Insight не проверяет файлы, загружаемые с надежных сайтов Интернета или внутренней сети. Надежные сайты настраиваются на вкладке **Панель управления Windows > Надежные интернет-сайты > Безопасность**. Когда включен параметр **Автоматически считать надежными файлы, загруженные с надежных сайтов Интернета или из внутренней сети**, клиент Symantec Endpoint Protection разрешает любые файлы, которые пользователь загружает с одного из надежных сайтов. Download Insight распознает только те надежные сайты, которые явно заданы вами или администратором. См. "Исключение объектов из сканирований" на стр. 71.

Задача	Описание
Настройка параметров Download Insight	Настройка параметров Download Insight может потребоваться по следующим причинам. ■ Требуется увеличение или уменьшение количества обнаружений Download Insight. Число обнаружений можно увеличить или уменьшить, настроив положение ползунка чувствительности к вредоносным файлам. На более низких уровнях чувствительности Download Insight обнаруживает меньше файлов, которые считает вредоносными, и больше неподтвержденных. При этом уменьшается число ложных срабатываний. На более высоких уровнях чувствительности Download Insight обнаруживает больше файлов, которые считает вредоносными, и меньше неподтвержденных. При этом увеличивается число ложных срабатываний. ■ Измените действие при обнаружении вредоносного или неподтвержденного файла. Можно изменить способ обработки вредоносных и неподтвержденных файлов в Download Insight. Действие для неподтвержденных файлов можно изменить, чтобы не получать уведомления об их обнаружении. ■ Получение предупреждений об обнаружениях Download Insight. Когда Download Insight обнаруживает файл, который считает вредоносным, на клиентском компьютере появляется сообщение, если для действия выбрано значение **Поместить в карантин**. Действие по помещению в карантин можно отменить. Когда компонент Download Insight обнаруживает файл, который он считает непроверенным, на клиентском компьютере отображается сообщение. Сообщение выводится, только когда для непроверенных файлов задано действие **Запросить** или **Карантин**. Если для действия выбрано значение **Запросить**, пользователь может разрешить или заблокировать файл. Если для действия выбрано значение **Поместить в карантин**, действие по помещению в карантин можно отменить. Можно выключить уведомление пользователей, чтобы не давать им возможность выбора при обнаружении компонентом Download Insight файла, считающегося неподтвержденным. Если вы включили уведомления, можно задать для непроверенных файлов действие **Игнорировать**, чтобы всегда пропускать такие обнаруженные угрозы и не уведомлять вас. Если уведомления включены, на число получаемых пользователями уведомлений будет влиять параметр чувствительности к вредоносным файлам. При повышении чувствительности увеличивается число уведомлений пользователя, поскольку при этом растет общее количество обнаружений. См. "Настройка параметров Download Insight" на стр. 62.

Задача	Описание
Управление тем, какие данные об обнаружениях репутации необходимо передавать в компанию Symantec	По умолчанию все управляемые клиенты отправляют сведения об обнаружениях репутации в компанию Symantec. Рекомендуется включить функцию отправки сведений об обнаружениях репутации. Предоставляемые сведения помогают компании Symantec бороться с новыми угрозами. См. "Основные сведения об отправке данных в Symantec в целях повышения безопасности вашего компьютера" на стр. 77.

Настройка параметров Download Insight

Настройка параметром Download Insight требуется в случае, если необходимо снизить количество ложных обнаружений на клиентских компьютерах. Можно изменить уровень чувствительности Download Insight к репутации файлов, которая используется для определения вредоносных файлов. Можно также изменить уведомление, отображаемое Download Insight на клиентских компьютерах в случае обнаружения угрозы.

Примечание: Чтобы компонент Download Insight работал, необходимо включить функцию автоматической защиты. Когда функция автоматической защиты выключена, компонент Download Insight не будет работать, даже если он включен.

См. "Управление обнаружениями Download Insight на компьютере" на стр. 58.

Как настроить параметры Download Insight

1. На боковой панели клиента нажмите **Изменить параметры**.
2. В разделе **Защита от вирусов и программ-шпионов** выберите **Настроить параметры**.
3. На вкладке **Download Insight** установите флажок **Включить Download Insight для обнаружения потенциальных угроз в загружаемых файлах на основе репутации файлов**.

   Если автоматическая защита выключена, компонент Download Insight не работает, даже если он включен.

4 Переместите ползунок, чтобы изменить чувствительность к вредоносным файлам.

Примечание: Если установлена только базовая защита от вирусов и программ-шпионов, для чувствительности к вредоносным файлам автоматически задается уровень 1 и вы не можете изменить эту настройку.

При установке более высокого уровня чувствительности Download Insight обнаруживает больше вредоносных файлов и считает меньшее количество файлов неподтвержденными. Однако более высокий уровень возвращает больше ложных срабатываний.

5 Включите или выключите следующие переключатели, чтобы использовать их в качестве дополнительного критерия при проверке неподтвержденных файлов:

- **Файлы с: *x* или менее пользователей**, где *x* по умолчанию равно 5. Можно выбрать другое значение в раскрывающемся списке.
- **Файлы, известные пользователям в течение: *x* или менее дней**, где *x* по умолчанию равно 2. Можно ввести любое значение
  Если неподтвержденные файлы отвечают этим критериям, Download Insight обнаруживает их как вредоносные.

6 Убедитесь, что установлен флажок **Автоматически считать надежными файлы, загруженные с веб-сайта внутренней сети**.

7 Щелкните **Действия**.

8 В разделе **Вредоносные файлы** укажите первое действие и второе действие.

9 В разделе **Неподтвержденные файлы** укажите действие.

10 Нажмите кнопку **ОК**.

11 Щелкните **Уведомления** и укажите, следует ли отображать уведомление, когда Download Insight обнаруживает угрозу.

Можно настроить текст предупреждающего сообщения.

12 Нажмите кнопку **ОК**.

Настройка параметров сканирования на наличие вирусов и программ-шпионов

По умолчанию Symantec Endpoint Protection обеспечивает компьютеру необходимую защиту от вирусов и угроз безопасности. В неуправляемых клиентах можно самостоятельно настраивать некоторые параметры сканирования.

Можно настроить заданное пользователем сканирование, глобальные параметры сканирования и параметры автоматической защиты.

- Настройка пользовательского сканирования
- Изменение параметров глобального сканирования
- Настройка автоматической защиты

См. "Управление сканированием на локальном компьютере" на стр. 35.

Настройка пользовательского сканирования

1. На боковой панели клиента выберите **Сканировать**.
2. На странице **Проверить на наличие угроз** щелкните правой кнопкой мыши нужное сканирование и выберите команду **Изменить**.
3. На вкладке **Параметры сканирования** выполните одно из следующих действий.
   - Чтобы указать типы сканируемых файлов, нажмите **Выбранные расширения**, затем нажмите кнопку **Расширения**.

     Примечание: Во время пользовательского сканирования всегда проверяются файлы-контейнеры, если в разделе **Дополнительные параметры сканирования** не отключен параметр проверки сжатых файлов при плановом сканировании или не созданы исключения для расширений файлов-контейнеров.

   - Для настройки первого и второго действия, предпринимаемых клиентом в отношении зараженного файла, выберите **Действия**.
   - Для настройки параметров уведомления выберите **Уведомления**.
     Уведомления, которые отображаются в пользовательском интерфейсе в стиле Windows 8, можно включать и отключать отдельно.
     См. "Управление всплывающими уведомлениями Symantec Endpoint Protection на компьютерах с Windows 8" на стр. 77.
   - Чтобы настроить дополнительные параметры для сжатых файлов, резервных копий и оптимизации, нажмите кнопку **Дополнительные параметры**.
     Для повышения быстродействия клиентского компьютера можно изменить параметры оптимизации.

   Дополнительную информацию о параметрах каждого диалогового окна можно получить, выбрав пункт **Справка**.
4. Нажмите кнопку **ОК**.

Изменение параметров глобального сканирования

1. На боковой панели клиента выберите пункт **Изменить параметры**, а затем рядом с функцией защиты от вирусов и программ-шпионов выберите команду **Настроить параметры**.
2. На вкладке **Глобальные настройки** в разделе **Параметры сканирования** измените функции эвристического поиска вирусов для Insight или Bloodhound.
3. Чтобы просмотреть или создать исключения из сканирования, щелкните **Показать список**. Завершив просмотр или создание исключений, нажмите кнопку **Закрыть**.
4. Внесите все необходимые изменения в разделы **Хранение журнала** или **Защита веб-браузера**.
5. Нажмите кнопку **ОК**.

Настройка автоматической защиты

1. На боковой панели клиента выберите **Изменить параметры**.
2. В разделе "Защита от вирусов и программ-шпионов" нажмите кнопку **Настроить параметры**.
3. На вкладке "Автоматическая защита" выполните следующие задачи.
   - Чтобы указать типы сканируемых файлов, щелкните **Выбранные**, затем нажмите кнопку **Расширения**.
   - Для настройки первого и второго действия, предпринимаемых клиентом в отношении зараженного файла, выберите **Действия**.
   - Для настройки параметров уведомления выберите **Уведомления**.

   Дополнительную информацию о параметрах каждого диалогового окна можно получить, выбрав пункт **Справка**.
4. На вкладке **Автоматическая защита** нажмите кнопку **Дополнительно**.

   Кроме того, можно настроить параметры кэша файлов и опции трассировщика угроз и резервных копий. Изменение этих параметров может помочь повысить производительность компьютера.
5. Щелкните **Сеть**, чтобы изменить настройки надежных файлов на удаленных компьютерах и настроить сетевой кэш.
6. Нажмите кнопку **ОК**.

Настройка действий при обнаружении вредоносных программ и угроз безопасности

В клиенте Symantec Endpoint Protection можно настроить действия, выполняемые при обнаружении вредоносной программы или угрозы безопасности. Можно настроить первое действие, а также второе действие, выполняемое в случае сбоя первого действия.

Примечание: Если компьютером управляет администратор и рядом с этими параметрами отображается значок замка, изменить их нельзя, потому что они заблокированы администратором.

Для всех типов сканирований действия настраиваются одинаковым образом. Для каждого сканирования действия настраиваются независимо. В разных сканированиях можно выбрать разные действия.

Примечание: Действия для Download Insight и SONAR настраиваются отдельно.

См. "Настройка параметров сканирования на наличие вирусов и программ-шпионов" на стр. 63.

См. "Настройка параметров Download Insight" на стр. 62.

См. "Изменение настроек SONAR" на стр. 82.

Дополнительную информацию о параметрах каждого диалогового окна можно получить, щелкнув **Справка**.

Как настроить действия при обнаружении вредоносных программ и угроз безопасности

1. На боковой панели клиента выберите **Изменить параметры**.
2. В разделе "Защита от вирусов и программ-шпионов" нажмите кнопку **Настроить параметры**, а затем на любой вкладке автоматической защиты щелкните **Действия**.
3. Щелкните **Действия**.
4. В диалоговом окне **Действия при сканировании** выберите категорию в разделах **Вредоносные программы** или **Угрозы безопасности**.

   Также можно выбрать подкатегорию. По умолчанию отдельные подкатегории автоматически настроены на применение действий, заданных для всей категории угроз безопасности.

   Категории изменяются динамически, по мере того как Symantec получает новую информацию об угрозах.

5 Для настройки действий только для подкатегории выполните одно из следующих действий.

- Включите переключатель **Переопределить действия, настроенные для вредоносных программ**, а затем настройте действия только для этой подкатегории.

  Примечание: В категории может быть всего одна подкатегория в зависимости от текущей классификации угроз компанией Symantec. Например, в разделе **Вредоносные программы** может быть одна подкатегория с названием **Вирусы**.

- Выберите **Переопределить действия для угроз безопасности**, а затем настройте действия только для этой подкатегории.

6 Выберите первое и второе действия для категории или подкатегории из следующих вариантов.

Исправить угрозу

Удаляет вирус из зараженного файла. Это первое действие по умолчанию для категории **Вредоносные программы**.

Примечание: Этот параметр доступен в качестве первого действия только для категории **Вредоносные программы**. Оно недоступно для угроз безопасности.

Этот вариант следует всегда выбирать в качестве основного действия для вирусов. Если клиент успешно удалит вирус из зараженного файла, никакие действия предпринимать не нужно. На вашем компьютере удалены все обнаруженные вирусы. Больше нет угрозы распространения этого вируса в другие области вашего компьютера.

Однако в некоторых случаях очищенный файл может оказаться непригодным к использованию. Это означает, что вирус слишком сильно повредил файл. Некоторые зараженные файлы исправить нельзя.

Примечание: Symantec Endpoint Protection не удаляет вредоносные программы, обнаруженные в приложениях и файлах, предназначенных для Windows 8. Вместо этого Symantec Endpoint Protection удаляет их.

Поместить угрозу в карантин	Перемещает зараженный файл в карантин. Вирусы из помещенных в карантин зараженных файлов теряют способность к распространению. ■ В случае обнаружения вредоносной программы это действие перемещает зараженный файл из исходного расположения в карантин. Этот параметр выбран по умолчанию в качестве второго действия для вредоносных программ. ■ В случае угроз безопасности это действие перемещает зараженные файлы из исходного расположения в карантин и пытается устранить побочные эффекты. Этот параметр выбран по умолчанию в качестве первого действия для угроз безопасности. Карантин содержит информацию обо всех выполненных действиях. При необходимости можно вернуть компьютер в состояние, в котором он находился до удаления угрозы клиентом. **Примечание:** Symantec Endpoint Protection не помещает в карантин вредоносные программы, обнаруженные в приложениях и файлах, предназначенных для Windows 8. Вместо этого Symantec Endpoint Protection удаляет их.
Удалить угрозу	Удаляет зараженный файл с жесткого диска компьютера. Если клиенту не удается удалить файл, в диалоговом окне **Уведомление** появятся сведения о предпринятом действии. Кроме того, эта информация будет сохранена в журнале событий. Этот параметр выбран по умолчанию в качестве второго действия для угроз безопасности. Используйте это действие только при наличии возможности заменить файл резервной копией, не содержащей вирусов или угроз безопасности. При обнаружении угрозы клиент безвозвратно удалит ее из системы. Зараженный файл нельзя будет восстановить из корзины. **Примечание:** Будьте осторожны при выборе этого действия для угроз безопасности. В некоторых случаях удаление угроз безопасности может привести к потере функциональности приложений.

Оставить как есть (занести в журнал)	Файл не изменяется, а в журнал угроз помещается запись для регистрации. Выберите этот параметр, чтобы вручную управлять тем, как клиент обрабатывает вредоносные программы или угрозы безопасности. **Примечание:** До выполнения дальнейших действий вредоносная программа может распространяться в другие области компьютера или на другие компьютеры в сети. Не выбирайте это действие при выполнении широкомасштабного автоматического сканирования, такого как плановое сканирование. Это действие позволяет просмотреть результаты сканирования и выполнить дополнительные действия позднее. Примером дополнительного действия может быть перемещение файла в карантин. Администратор может настроить сообщение с инструкциями по противодействию угрозам, отправляемое при обнаружении угрозы или вируса.

7 Повторите эти шаги для каждой категории вирусов или угроз, которая должна обрабатываться особым способом, и нажмите кнопку **OK**.

8 Если была выбрана категория угроз безопасности, то можно настроить пользовательские действия для отдельных элементов этой категории. Кроме того, можно исключить угрозу безопасности из сканирования. Например, можно исключить программу показа рекламы, применяемую для работы.

9 Нажмите кнопку **OK**.

Сведения об исключении объектов из сканирования

Исключения — это файлы и другие объекты, которые необходимо исключить из сканирований. Если пользователь знает, что некоторые файлы заведомо безопасны, то такие файлы также можно исключить из процесса сканирования. В некоторых случаях исключения помогают ускорить сканирование и повысить производительность системы. Как правило, исключения создавать не требуется.

В управляемых клиентах исключения из сканирований пользователей может создавать администратор. Если исключение, настроенное пользователем, конфликтует с исключением, заданным администратором, то будет применяться второе. Администратор может также запретить пользователю настраивать любой или все типы исключений.

Табл. 3-9 Типы исключений

Тип исключения	Описание
Файл	Применимо к плановым сканированиям, сканированиям вручную, автоматической защите, SONAR и управлению приложениями. Выбранные файлы игнорируются при сканировании.
Папка	Применимо к плановым сканированиям, сканированиям вручную, автоматической защите, SONAR и управлению приложениями. Выбранные папки игнорируются при сканировании.
Известные угрозы	Применимо к плановым сканированиям, сканированиям вручную, автоматической защите и SONAR. Любые выбранные угрозы игнорируются при сканировании.
Расширения	Применимо к плановым сканированиям, сканированиям вручную и автоматической защите. Любые файлы с указанными расширениями игнорируются при сканировании.
Веб-домен	Применимо к Download Insight. Download Insight игнорирует указанный надежный веб-домен.
Приложение	Применимо к плановым сканированиям, сканированиям вручную, автоматической защите, SONAR и Download Insight. Указанное здесь приложение сканирования игнорируют, регистрируют в журнале, помещают в карантин или прерывают.
Изменение в настройках DNS или файле hosts	Применимо к сканированию SONAR. Когда указанное приложение пытается изменить настройки DNS или файл hosts, операции сканирования игнорируют, регистрируют в журнале или блокируют приложение или запрашивают пользователя.

Примечание: Если в почтовой программе вся электронная почта хранится в одном файле, то следует создать исключение для файла "Входящие". По умолчанию сканирования помещают вирусы в карантин. Если сканирование обнаружит вирус в файле "Входящие", в карантин будет помещен весь файл. Это приведет к тому, что почта станет недоступна.

См. "Исключение объектов из сканирований" на стр. 71.

Исключение объектов из сканирований

Можно исключать заведомо безопасные приложения и файлы из процесса сканирования. Кроме того, можно исключать некоторые объекты из сканирования для повышения быстродействия компьютера.

В управляемых клиентах исключения из сканирований пользователей может создавать администратор. Если исключение, настроенное пользователем, конфликтует с исключением, заданным администратором, то будет применяться второе.

Можно исключать объекты из сканирований на наличие угроз безопасности, исключать папки из сканирований SONAR, а также исключать приложения из любых видов сканирования.

- Как исключить объекты из сканирований угроз безопасности
- Как исключить папку из сканирования SONAR
- Как исключить приложение, изменяющее DNS или файл хоста
- Как изменить способ обработки приложения всеми сканированиями

Примечание: Если установлены только основные серверные компоненты Windows Server 2008, внешний вид диалоговых окон может отличаться от внешнего вида окон, описанных в этих процедурах.

Как исключить объекты из сканирований угроз безопасности

1. На боковой панели клиента выберите **Изменить параметры**.
2. Рядом с пунктом **Исключения** выберите команду **Настроить параметры**.
3. В диалоговом окне **Исключения**, в разделе **Исключения пользователя** выберите **Добавить > Исключения угроз безопасности**.
4. Выберите один из следующих типов исключений:
   - **Известные угрозы**
   - **Файл**
   - **Папка**
   - **Расширения**
   - **Веб-домен**
5. Выполните одно из следующих действий.
   - Включите переключатели для тех известных угроз безопасности, которые нужно исключить из сканирования.

Чтобы регистрировать события обнаружения и игнорирования угроз безопасности в журнале, установите флажок **Добавлять в журнал запись при обнаружении угрозы**.

- Для файлов или папок: выберите файл или папку, которые необходимо исключить, или введите имя файла или папки.
  Выберите тип сканирования (**Все сканирования**, **Автоматическая защита** или **Запланировано/по требован.**) и нажмите кнопку **ОК**.
  При выполнении приложения, которое записывает в папку много временных файлов, может потребоваться исключить эту папку из области действия функции автоматической защиты. Функция автоматической защиты сканирует записываемые файлы, поэтому можно повысить быстродействие компьютера, ограничив исключение операциями планового сканирования и сканирования по требованию.
  Из операций планового сканирования и сканирования по требованию может потребоваться исключить папки, которые редко используются либо содержат архивированные или упакованные файлы. Например, плановое сканирование или сканирование по требованию файлов с высокой степенью архивирования, которые редко используются, может снизить быстродействие компьютера. Функция автоматической защиты по-прежнему будет защищать эту папку, выполняя сканирование только при доступе к файлам или их записи в папку.
- Для расширений файлов укажите расширение, которое нужно исключить.
  В текстовом поле можно указать только одно расширение. Если указать несколько расширений, клиент будет рассматривать их как одно длинное расширение.
- Для доменов, которые требуется исключить из обнаружения Download Insight и SONAR, введите имя домена или IP-адрес. Можно указать URL-адрес, но для исключения будет использоваться только часть URL-адреса, относящаяся к домену. При указании URL-адреса к нему можно добавить префикс HTTP или HTTPS (не зависит от регистра), но исключение будет применяться для обоих вариантов. Исключение позволит вам загружать файлы из любого расположения в домене.
  При работе с Download Insight можно использовать символы подстановки, но при этом диапазоны немаршрутизируемых IP-адресов не поддерживаются. Например, Download Insight не может распознать 10.*.*.* как надежный сайт. Download Insight также не поддерживает сайты, которые обнаруживаются с помощью параметра **Свойства обозревателя > Безопасность > Автоматически определять принадлежность к интрасети**.

6 Нажмите кнопку **ОК**.

Как исключить папку из сканирования SONAR

1 На боковой панели клиента выберите **Изменить параметры**.

2 Рядом с пунктом **Исключения** выберите команду **Настроить параметры**.

3 В диалоговом окне **Исключения** в разделе **Исключения пользователя** щелкните **Добавить > Исключение SONAR > Папка**.

4 Выберите папку, которую нужно исключить, установите или снимите флажок **Включая подпапки** и нажмите кнопку **OK**.

5 Нажмите кнопку **Закрыть**.

Как исключить приложение, изменяющее DNS или файл хоста

1 На боковой панели клиента выберите **Изменить параметры**.

2 Рядом с пунктом **Исключения** выберите команду **Настроить параметры**.

3 В диалоговом окне **Исключения** в разделе **Исключения пользователя** выберите **Исключение изменения DNS или файла хоста > Приложение**

4 Выберите приложение, которое необходимо исключить, а затем нажмите кнопку **OK**.

Как изменить способ обработки приложения всеми сканированиями

1 На боковой панели клиента выберите **Изменить параметры**.

2 Рядом с пунктом **Исключения** выберите команду **Настроить параметры**.

3 В диалоговом окне **Исключения**, в разделе **Исключения пользователя** выберите **Добавить > Исключение приложения**.

4 Выберите имя файла приложения.

5 В раскрывающемся списке **Действие** выберите **Игнорировать**, **Занести в журнал**, **Карантин**, **Прервать** или **Удалить**.

6 Нажмите кнопку **OK**.

7 Нажмите кнопку **Закрыть**.

См. "Управление сканированием на локальном компьютере" на стр. 35.

См. "Сведения об исключении объектов из сканирования" на стр. 69.

Управление файлами, помещенными в карантин, на компьютере

Сведения о помещенных в карантин файлах

По умолчанию Symantec Endpoint Protection пытается очистить зараженный файл от обнаруженного вируса. Если очистить файл не удается, операция сканирования помещает этот файл в карантин локального компьютера. Когда клиент перемещает зараженный файл в карантин, он зашифровывает этот файл. Поскольку файл, помещенный в карантин, зашифрован, вы не сможете получить к нему доступ. Файл, находящийся в

карантине, не может заразить другие файлы на вашем компьютере или на компьютерах в сети. Однако при помещении файла в карантин не происходит исправление угрозы. Она остается на компьютере до тех пор, пока клиент не удалит угрозу или сам файл.

После обновления описаний вирусов на компьютере клиент автоматически выполняет повторное сканирование файлов в карантине. В некоторых случаях после обновления описаний удается очистить или исправить файлы, ранее помещенные в карантин.

- Большинство вирусов можно поместить в карантин. Загрузочные вирусы, как правило, заражают загрузочный сектор или таблицу разделов, а эти элементы переместить в карантин нельзя. Иногда клиент обнаруживает неизвестный вирус, который не удается устранить с помощью текущего набора описаний вирусов.
- При обнаружении угроз безопасности зараженные файлы помещаются в карантин, поэтому побочные эффекты угрозы устраняются.
- Компоненты Download Insight и SONAR также могут помещать файлы в карантин.

См. "Как функция сканирования реагирует на обнаружение вируса или угрозы" на стр. 49.

Управление файлами в карантине

Поскольку в карантине обрабатываются только зараженные файлы на вашем компьютере, вы можете оставить файлы в карантине. Однако есть ряд действий, которые может потребоваться выполнить с файлом в карантине. Например, если файл был помещен в карантин по ошибке, можно восстановить его из карантина. Или при необходимости экономии места на компьютере можно уменьшить время до автоматического удаления содержимого в карантине.

Как управлять файлами в карантине

1. На боковой панели клиента выберите команду **Показать карантин**.
2. В окне **Показать карантин** выберите файл в списке объектов, помещенных в карантин.
3. Выберите один из вариантов и следуйте инструкциям, выводимым на экран.

См. "Управление сканированием на локальном компьютере" на стр. 35.

Включение автоматической защиты

Не рекомендуется выключать автоматическую защиту для файлов и процессов, электронной почты Интернета и почтовых приложений рабочих групп. Если какая-либо разновидность автоматической защиты выключена, значок состояния защиты от вирусов и программ-шпионов на странице состояния будет показан красным цветом.

В управляемых клиентах администратор может заблокировать функцию автоматической защиты. Тогда пользователь не сможет ее выключить. Также администратор может

указать, что после временного выключения автоматическая защита должна автоматически восстанавливаться через указанный период времени.

Примечание: При отключении автоматической защиты также отключается компонент Download Insight, даже если он был включен. Компонент SONAR также не сможет обнаруживать угрозы эвристически, но продолжит обнаруживать изменения файл хоста и системы.

Предупреждение! Согласно рекомендации Symantec при поиске неполадок на клиентском компьютере автоматическую защиту следует выключать только на время.

Как включить автоматическую защиту для файловой системы

- На странице **Состояние** клиента в разделе **Защита от вирусов и программ-шпионов** выполните одно из следующих действий.
  - Щелкните **Параметры > Включить защиту от вирусов и программ-шпионов**.
  - Выберите **Параметры > Выключить все компоненты защиты от вирусов и программ-шпионов**.

Как включить автоматическую защиту для электронной почты

1. На боковой панели клиента нажмите **Изменить параметры**.
2. В разделе **Защита от вирусов и программ-шпионов** щелкните **Настроить параметры**.
3. Выполните одно из следующих действий.
   - На вкладке **Автоматическая защита Интернет-почты** установите флажок **Включить автоматическую защиту интернет-почты**.
   - На вкладке **Автоматическая защита Microsoft Outlook** установите флажок **Включить автоматическую защиту Microsoft Outlook**.
   - На вкладке **Автоматическая защита Lotus Notes** установите флажок **Включить автоматическую защиту Lotus Notes**.

   Серверные операционные системы не поддерживают автоматическую защиту интернет-почты. Автоматическая защита Microsoft Outlook автоматически устанавливается на компьютерах, где выполняется Outlook.
4. Нажмите кнопку **ОК**.

См. "Сведения о типах автоматической защиты" на стр. 47.

См. "Как с помощью значков на странице "Состояние" определить, защищен ли клиентский компьютер" на стр. 17.

Включение и отключение раннего запуска защиты от вредоносных программ

Ранний запуск защиты от вредоносных программ (ELAM) обеспечивает защиту компьютеров при их запуске до момента инициализации сторонних драйверов. Вредоносные программы, которые могут загружаться в качестве драйвера, или руткиты могут совершать атаки раньше, чем полностью загрузится операционная система и запустится клиент. Руткиты иногда могут скрывать себя от средств сканирования на вирусы и программы-шпионы. Ранний запуск защиты от вредоносных программ позволяет при запуске обнаруживать руткиты и неблагонадежные драйверы.

Symantec Endpoint Protection предоставляет драйвер раннего запуска защиты от вредоносных программ, который обеспечивает защиту вместе с драйвером Microsoft для раннего запуска защиты от вредоносных программ. Эти настройки поддерживаются в Microsoft Windows 8 и более поздних версий, а также в Windows Server 2012 и более поздних версий. Чтобы этот параметр вступил в силу, необходимо включить драйвер Windows для раннего запуска защиты от вредоносных программ.

Примечание: Нельзя создать исключения для отдельных обнаружений ELAM, однако можно создать глобальное исключение для занесения в журнал всех неблагонадежных драйверов в качестве неизвестных.

Для исправления некоторых обнаружений ELAM может потребоваться запуск модуля Power Eraser. Power Eraser входит в состав средства Symantec Help. Чтобы получить средство Symantec Help, нажмите кнопку **Справка** в клиенте Symantec Endpoint Protection.

Как включить или выключить ранний запуск защиты от вредоносных программ

1. На боковой панели клиента нажмите **Изменить параметры**.
2. В разделе **Защита от вирусов и программ-шпионов** выберите **Настроить параметры**.
3. На вкладке **Ранний запуск защиты от вредоносных программ** включите или выключите переключатель **Включить ранний запуск защиты**.
4. Если требуется только регистрировать обнаружения в журнале, в разделе **Когда обнаружен потенциально опасный драйвер** выберите вариант **Записывать обнаружение как неизвестное, чтобы загрузка драйвера была разрешена Windows**.
5. Нажмите кнопку **ОК**.

См. "Управление сканированием на локальном компьютере" на стр. 35.

См. "Устранение неполадок на компьютере с помощью средства Symantec Diagnostic Tool (SymDiag)" на стр. 116.

См. "Исключение объектов из сканирований" на стр. 71.

Управление всплывающими уведомлениями Symantec Endpoint Protection на компьютерах с Windows 8

По умолчанию в пользовательском интерфейсе в стиле Windows 8 и на рабочем столе Windows 8 отображаются всплывающие уведомления с сообщениями об обнаружениях вредоносных программ и других важных событиях Symantec Endpoint Protection.

Осуществлять управление всплывающими уведомлениями можно следующими способами:

- В клиенте на странице **Параметры управления клиентами** измените глобальный параметр для уведомлений пользовательского интерфейса в стиле Windows 8.
- В Windows 8 измените параметры уведомлений для операционной системы. Уведомления Symantec Endpoint Protection появляются только в том случае, если в Windows 8 задано их отображение. Дополнительные сведения приведены в пользовательской документации Windows 8.

В управляемых клиентах администратор может включать и выключать всплывающие уведомления в Windows 8.

См. "Реагирование на всплывающие уведомления Symantec Endpoint Protection, отображаемые на компьютерах с Windows 8" на стр. 30.

Основные сведения об отправке данных в Symantec в целях повышения безопасности вашего компьютера

По умолчанию клиент периодически отправляет анонимную информацию о найденных угрозах, характеристиках сети и параметрах конфигурации в компанию Symantec. Symantec использует эти сведения для защиты клиентских компьютеров от новых, целенаправленных и меняющихся угроз. Любые отправляемые вами данные расширяют возможности Symantec в борьбе с угрозами. Компания Symantec рекомендует отправлять максимально возможный объем информации.

Symantec каждый раз старается обезличить данные, отправляемые клиентами.

Анонимная информация, отправляемая клиентом в Symantec, дает следующие преимущества:

- Повышение безопасности сети

- Оптимизация быстродействия продукта

Но в некоторых случаях может потребоваться отключить отправку этой информации с клиента. Например, вместо полного отключения отправок клиента можно запретить отправку только информации о сети.

Примечание: Компания Symantec рекомендует не отключать отправку сведений клиентами. Выключение отправки может помешать быстрому обнаружению и устранению ложных срабатываний в приложениях, используемых только в вашей организации. Не имея на руках информации о вредоносных программах в вашей организации, службе поддержки Symantec потребуется больше времени, чтобы отреагировать на угрозы.

Как изменить параметры отправки в Symantec

1. Выберите **Изменить параметры** > **Управление клиентом**.
2. На вкладке **Отправка** установите флажок **Отправить анонимные данные в Symantec, чтобы получить расширенный анализ защиты от угроз**. Этот параметр позволяет Symantec Endpoint Protection отправлять информацию об угрозах, обнаруженных на компьютере, а также информацию о сети и конфигурации.

   Symantec не рекомендует отключать этот параметр.
3. Выберите **Дополнительные параметры**, чтобы выбрать типы сведений для отправки.
4. Нажмите кнопку **ОК**.

Можно также вручную отправить в Symantec файл из карантина.

См. "Управление файлами, помещенными в карантин, на компьютере" на стр. 73.

Дополнительную информацию о конфиденциальности см. в следующем документе:

Заявление о конфиденциальности

Применение клиента вместе с центром обеспечения безопасности Windows

Если в системе Windows XP с пакетом обновления 2 или 3 используется Центр обеспечения безопасности Windows (WSC), в его окне отображается состояние Symantec Endpoint Protection.

В Табл. 3-10 указано состояние системы защиты, которое может быть показано в WSC.

Табл. 3-10 Состояние системы защиты в WSC

Состояние продукта Symantec	Состояние системы защиты
Продукт Symantec Endpoint Protection не установлен	Не найдена (красный)
Продукт Symantec Endpoint Protection установлен с полным набором компонентов защиты	Включена (зеленый)
Продукт Symantec Endpoint Protection установлен, но описания вирусов и угроз устарели	Устарела (красный)
Продукт Symantec Endpoint Protection установлен, но автоматическая защита файловой системы выключена	Выключена (красный)
Продукт Symantec Endpoint Protection установлен, но автоматическая защита файловой системы выключена, а описания вирусов и угроз устарели	Выключена (красный)
Продукт Symantec Endpoint Protection установлен, но функция ccSvcHst была вручную выключена	Выключена (красный)

Табл. 3-11 содержит перечень состояний брандмауэра Symantec Endpoint Protection в WSC.

Табл. 3-11 Состояние брандмауэра в WSC

Состояние продукта Symantec	Состояние брандмауэра
Брандмауэр Symantec не установлен	Не найден (красный)
Брандмауэр Symantec установлен и включен	Включен (зеленый)
Брандмауэр Symantec установлен, но выключен	Выключен (красный)
Брандмауэр Symantec не установлен или выключен, либо установлен и включен другой брандмауэр	Включена (отмечено зеленым цветом)

Примечание: В Symantec Endpoint Protection брандмауэр Windows выключается по умолчанию.

Если включено несколько брандмауэров, то WSC сообщит о наличии нескольких брандмауэров.

Сведения о SONAR

SONAR — это защита в реальном времени, обнаруживающая потенциально вредоносные приложения при их запуске на компьютерах. SONAR предоставляет защиту "с нулевой задержкой", поскольку обнаруживает угрозы раньше, чем для борьбы с ними будут созданы определения стандартного обнаружения вирусов и программ-шпионов.

Для обнаружения новых и неизвестных угроз SONAR использует как эвристические алгоритмы, так и анализ данных о репутации. SONAR обеспечивает дополнительный уровень защиты клиентских компьютеров и расширяет возможности имеющихся технологий: защиту от вирусов и программ-шпионов, предотвращение вторжений, предупреждение последствий использования эксплойтов памяти и защиту с помощью брандмауэра

SONAR применяет систему эвристик, которая для обнаружения неизвестных угроз использует интерактивную аналитическую сеть Symantec с превентивным мониторингом на компьютере пользователя. SONAR обнаруживает также изменения в поведении контролируемого компьютера пользователя.

Примечание: Автоматическая защита для обнаружения подозрительного поведения в файлах также применяет эвристический метод, известный как технология Bloodhound.

SONAR может вставлять определенный код в приложения, выполняемые в режиме пользователя Windows, чтобы отслеживать их возможную подозрительную активность. В некоторых случаях это может снизить быстродействие приложений или привести к проблеме с их запуском. Создав исключение, можно исключить файл, папку или приложение из такого типа отслеживания.

SONAR обнаруживает угрозы не по типу приложения, а по поведению процесса. SONAR воздействует на приложение только при его вредоносном поведении, независимо от типа приложения. Например, SONAR не обнаружит троянского коня или клавиатурного шпиона, если их поведение не является вредоносным.

SONAR обнаруживает следующие объекты.

Эвристические угрозы	SONAR использует эвристики, чтобы определить, ведет ли себя неизвестный файл подозрительно и насколько высока угроза, которую он может представлять. Кроме того, он использует данные о репутации, чтобы определить угрозу как весьма вероятную или маловероятную.
Изменения системы	SONAR обнаруживает приложения или файлы, пытающиеся изменить параметры DNS или файл хоста на клиентском компьютере.

Надежные приложения с неадекватным поведением	Некоторые нормальные надежные файлы могут быть связаны с подозрительным поведением. SONAR обнаруживает такие файлы как события подозрительного поведения. Например, популярное приложение для совместной работы с документами может создавать исполняемые файлы.

Отключение автоматической защиты ограничит возможности SONAR по обнаружению файлов с весьма вероятной или маловероятной угрозой. Отключение запросов Insight (запросов о репутации) может также привести к ограничению возможностей обнаружения SONAR.

Примечание: SONAR не вставляет код в приложения на компьютерах с Symantec Endpoint Protection версий, предшествующих 12.1.2. Если для управления клиентами используется Symantec Endpoint Protection Manager 12.1.2 или более поздних версий, исключение файла SONAR в политике исключений на таких устаревших клиентах игнорируется. При использовании устаревшего Symantec Endpoint Protection Manager для управления клиентами устаревшая политика не поддерживает исключения файла SONAR для клиентов Symantec Endpoint Protection 12.1.2. Однако можно запретить вставку кода SONAR в приложения в этих клиентах, создав исключение **Приложение для мониторинга** в устаревшей политике. После того как клиент обнаружит приложение, можно настроить исключение приложения в политике.

См. "Управление SONAR на вашем компьютере" на стр. 81.

См. "Исключение объектов из сканирований" на стр. 71.

Управление SONAR на вашем компьютере

Компонент SONAR управляется как часть превентивной защиты от угроз. В управляемых клиентах некоторые параметры могут быть заблокированы администратором.

Табл. 3-12 Управление SONAR на вашем компьютере

Задача	Описание
Убедитесь, что компонент SONAR включен	Для обеспечения наилучшей защиты клиентского компьютера компонент SONAR необходимо включить. По умолчанию компонент SONAR включен. Включение компонента SONAR происходит при включении превентивной защиты от угроз. См. "Включение защиты на клиентском компьютере" на стр. 114.

Задача	Описание
Убедитесь, что запросы Insight включены.	При обнаружении угроз SONAR использует данные репутации в дополнение к эвристикам. Отключение запросов Insight (запросов о репутации) может также привести к использованию SONAR только эвристических методов обнаружения. При этом может увеличиться число ложных срабатываний, а защита, предоставляемая SONAR, будет ограничена. См. "Настройка параметров Download Insight" на стр. 62.
Измените настройки SONAR	SONAR можно включить или выключить. Кроме того, можно изменить действие, выполняемое SONAR при обнаружении угроз некоторых типов. Изменение действия при обнаружении угрозы может потребоваться для снижения числа ложных обнаружений. См. "Изменение настроек SONAR" на стр. 82.
Создайте исключения для заведомо безопасных приложений	SONAR может обнаруживать файлы и приложения, которые требуется выполнить на компьютере. Можно создать исключения SONAR для файлов, папок или приложений на странице **Исключения > Изменить параметры**. Можно также создать исключение для карантина. См. "Исключение объектов из сканирований" на стр. 71.
Предотвращение проверки некоторых приложений модулем SONAR	В ряде случаев, когда SONAR вставляет код в приложение для его проверки, приложение может стать нестабильным или перестать запускаться. Для приложения можно создать исключение файла или приложения. См. "Исключение объектов из сканирований" на стр. 71.
Отправьте сведения об обнаружениях SONAR в Symantec Security Response	Компания Symantec рекомендует отправлять сведения об обнаружениях в Symantec Security Response. Предоставляемые сведения помогают компании Symantec бороться с новыми угрозами. Отправка включена по умолчанию. См. "Основные сведения об отправке данных в Symantec в целях повышения безопасности вашего компьютера" на стр. 77.

См. "Управление сканированием на локальном компьютере" на стр. 35.

См. "О типах сканирований" на стр. 44.

Изменение настроек SONAR

Изменение действий SONAR может потребоваться для снижения числа ложных обнаружений. Кроме того, можно изменить уведомления для эвристических обнаружений SONAR.

Примечание: В управляемых клиентах эти параметры могут быть заблокированы администратором.

Изменение настроек SONAR

1. На боковой панели клиента щелкните **Изменить параметры**.
2. Рядом с пунктом **Превентивная защита** нажмите кнопку **Настроить параметры**.
3. На вкладке **SONAR** измените действия для эвристически обнаруживаемых угроз с высокой или низкой степенью риска.

   Для обнаружения маловероятных угроз можно включить агрессивный режим. Это увеличит уровень чувствительности SONAR для обнаружении незначительных угроз. Он может привести к увеличению числа ложных срабатываний.

   Кроме того, можно изменить параметры уведомлений и указать, работает ли модуль SONAR на удаленных компьютерах (сетевых дисках).
4. На вкладке **Обнаружение подозрительного поведения** измените действие при обнаружении весьма вероятных или маловероятных угроз. Модуль SONAR обнаруживает эти угрозы, если надежные файлы связаны с подозрительным поведением.

   Обнаружение подозрительного поведения можно включить или отключить, только когда выключен SONAR.
5. На вкладке **События по изменению системы** измените действие сканирования при обнаружении попыток изменить параметры сервера DNS или файл хоста.
6. Нажмите кнопку **ОК**.

См. "Управление SONAR на вашем компьютере" на стр. 81.

Проверка соблюдения требований безопасности с помощью сканирования целостности хоста

Сканирование целостности хоста перед подключением компьютера к сети подтверждает его соответствие определенным требованиям безопасности. Например, при проверке целостности хоста может определяться наличие последнего исправления безопасности операционной системы. Если компьютер не соответствует требованиям безопасности, клиент может выполнить исправление компьютера, чтобы обеспечить успешное прохождение проверки целостности хоста. Для исправления операция проверки автоматически загружает и устанавливает необходимое программное обеспечение. Администратор может отправить пользователю сообщение о необходимости выполнить исправление компьютера.

Проверка целостности хоста начинает выполняться при запуске компьютера и продолжается до момента завершения сетевого подключения. Проверку целостности хоста также можно выполнить вручную.

Кроме того, администратор может настроить проверку целостности хоста так, чтобы она считалась пройденной даже в случае несоблюдения какого-либо требования. Результаты проверок целостности хоста можно просматривать в журнале безопасности клиента.

Как проверить соблюдение требований безопасности с помощью сканирования целостности хоста

1. На боковой панели клиента щелкните **Сканировать**.
2. В диалоговом окне **Сканировать** щелкните **Выполнить сканирование целостности хоста**.
3. Нажмите кнопку **ОК**.

   Если несоответствие требованиям препятствует доступу к сети, следует восстановить доступ посредством обновления компьютера для обеспечения соответствия требованиям.

   Результаты сканирования отображаются в журнале безопасности.

См. "Исправление компьютера для прохождения проверки целостности" на стр. 84.

См. "Просмотр журналов" на стр. 119.

Исправление компьютера для прохождения проверки целостности

Если клиент не соответствует требованиям политики целостности хоста, применяется один из следующих способов.

- Клиент автоматически загружает обновление программы.
- Клиент предлагает пользователю загрузить обновление.

Как исправить компьютер

- В появившемся окне Symantec Endpoint Protection выполните одно из следующих действий:
  - Чтобы узнать, какие требования к безопасности не выполнены, щелкните **Сведения**.
  - Чтобы немедленно установить ПО, нажмите кнопку **Восстановить сейчас**. В некоторых случаях начатую процедуру установки можно отменить.
  - Чтобы приостановить установку программы, нажмите **Напомнить позже** и выберите промежуток времени в раскрывающемся списке. Администратор может указать, сколько раз установка может быть приостановлена.

См. "Проверка соблюдения требований безопасности с помощью сканирования целостности хоста" на стр. 83.

Включение защиты от изменений

Функция защиты от изменений обеспечивает постоянную защиту приложений Symantec, работающих на серверах и клиентах. Она предотвращает изменение ресурсов Symantec угрозами безопасности. Защиту от изменений можно включать и выключать по своему усмотрению. Можно также настроить действие, которое будет выполнять функция защиты от изменений при обнаружении попытки изменения ресурсов Symantec на компьютере пользователя.

По умолчанию для защиты от изменений выбрано значение **Блокировать и не вносить в журнал**.

Примечание: Настройка защиты от изменений для управляемых клиентов может быть заблокирована администратором.

Как включить защиту от изменений

1. На боковой панели клиента выберите **Изменить параметры**.
2. В разделе **Управление клиентом** нажмите кнопку **Настроить параметры**.
3. Убедитесь, что на вкладке **Защита от изменений** установлен флажок **Защита продукта Symantec по обеспечению безопасности от изменения или завершения**.
4. В списке **Действие при попытке приложения изменить или завершить программу обеспечения безопасности Symantec** выберите **Заносить в журнал**, **Блокировать и не вносить в журнал** или **Блокировать и внести в журнал**.
5. Нажмите кнопку **ОК**.

Глава 4

Управление брандмауэром, предотвращением вторжений и усилением защиты приложений

В этой главе рассмотрены следующие вопросы:

- Управление защитой с помощью брандмауэра
- Управление правилами брандмауэра
- Настройка параметров брандмауэра
- Разрешение и блокировка доступа приложений к сети
- Разрешение и блокировка приложений, которые уже запущены на клиенте
- Блокирование трафика при включении экранной заставки или когда не запущен брандмауэр
- Настройка предотвращения вторжений
- Предотвращение атак на уязвимые приложения

Управление защитой с помощью брандмауэра

По умолчанию клиент Symantec Endpoint Protection обеспечивает надлежащий уровень защиты брандмауэром, необходимый компьютеру. Однако администратор может изменить некоторые стандартные параметры и правила брандмауэра.

Если администратор предоставил возможность изменять защиту брандмауэром, можно изменить правила или параметры брандмауэра

Табл. 4-1 содержит список задач брандмауэра, которые можно выполнить для защиты компьютера. Все эти задачи не являются обязательными и могут выполняться в любом порядке.

Табл. 4-1 Управление защитой с помощью брандмауэра

Задача	Описание
Изучение работы брандмауэра	Выясните, как брандмауэр защищает компьютер от атак из сети. См. "Принципы работы брандмауэра" на стр. 88.
Добавление и настройка правил брандмауэра	Можно добавлять новые правила брандмауэра и изменять существующие. Например, может потребоваться заблокировать приложение, выполнение которого на компьютере нежелательно (программа показа рекламы). См. "Управление правилами брандмауэра" на стр. 89. Кроме того, можно настраивать правила брандмауэра, чтобы разрешать или запрещать приложениям доступ к сети. См. "Разрешение и блокировка приложений, которые уже запущены на клиенте" на стр. 101.
Настройка параметров брандмауэра	Дополнительно к созданию правил брандмауэра можно включить и настроить параметры брандмауэра для дальнейшего усиления защиты. См. "Настройка параметров брандмауэра" на стр. 96.
Просмотр журналов брандмауэра	Проверка состояния защиты брандмауэра на локальном компьютере позволяет узнать следующее: ■ правильность работы созданных правил брандмауэра; ■ наличие атак из сети, заблокированных клиентом; ■ наличие заблокированных клиентом приложений, которые должны были выполняться. Состояние защиты брандмауэром можно проверить с помощью журналов трафика и пакетов. По умолчанию журнал пакетов отключен на управляемых клиентах. См. "Сведения о журналах" на стр. 117. См. "Включение журнала пакетов" на стр. 119.

Задача	Описание
Разрешение или блокирование приложений и определенных видов трафика	Для обеспечения дополнительной безопасности можно блокировать сетевой трафик для компьютера в следующих ситуациях. ■ Можно блокировать трафик при включенной экранной заставке компьютера. ■ Можно блокировать трафик на время, когда не запущен брандмауэр. ■ Можно постоянно и полностью блокировать трафик. См. "Блокирование трафика при включении экранной заставки или когда не запущен брандмауэр" на стр. 102. ■ Можно либо автоматически разрешать или блокировать доступ к сети приложению, работающему на вашем компьютере, либо запрашивать пользователя о необходимом действии. Параметры, которые можно настроить дополнительно См. "Разрешение и блокировка доступа приложений к сети" на стр. 100. См. "Разрешение и блокировка приложений, которые уже запущены на клиенте" на стр. 101.
Включение или отключение брандмауэра	Если требуется устранить неполадку, можно временно выключить защиту от сетевых угроз. Например, ее отключение может потребоваться для того, чтобы затем открыть определенное приложение. См. "Включение защиты на клиентском компьютере" на стр. 114.

Принципы работы брандмауэра

Брандмауэр выполняет следующие задачи.

- Предотвращает любой несанкционированный доступ к корпоративным компьютерам и сетям, подключенным к Интернету.
- Отслеживает взаимодействие компьютера с другими компьютерами в Интернете.
- Создает щит, разрешающий или блокирующий доступ к информации на компьютере
- Предупреждает о попытках подключения других компьютеров.
- Предупреждает пользователя о всех попытках локальных программ подключиться к другим компьютерам.

Брандмауэр просматривает пакеты данных, проходящие через Интернет. Пакет — это отдельный блок данных, являющийся частью потока данных между двумя компьютерами. В месте назначения пакеты снова объединяются в один непрерывный поток данных.

В пакеты включены указанные ниже сведения о данных.

- Исходный компьютер
- Получатель или получатели
- Способ обработки данных пакета

- Порты для приема пакетов
  Порты — это каналы, разделяющие поток данных, приходящий из сети Интернет. Порты прослушиваются приложениями, выполняемыми на компьютере. Приложения принимают данные, переданные в порты.

Для атак из сети используются уязвимости в незащищенных приложениях. Злоумышленники используют эти уязвимости для отправки пакетов с вредоносным кодом на определенный порт. Когда уязвимое приложение прослушивает порты, вредоносный код позволяет злоумышленникам получить доступ к компьютеру.

См. "Управление защитой с помощью брандмауэра" на стр. 87.

Управление правилами брандмауэра

Правила брандмауэра определяют, как брандмауэр защищает компьютеры от вредоносного входящего трафика и приложений. Брандмауэр проверяет все входящие и исходящие пакеты на соответствие включенным пользователем правилам. Он разрешает или блокирует пакеты на основании условий, указанных в правилах брандмауэра.

В состав клиента Symantec Endpoint Protection входят стандартные правила брандмауэра для защиты компьютера. При этом для обеспечения дополнительной защиты пользователь может изменять правила брандмауэра, если это разрешено администратором и если клиент является неуправляемым.

Табл. 4-2 описывает то, что нужно знать для управления правилами брандмауэра.

Табл. 4-2 Управление правилами брандмауэра

Задача	Описание
Сведения о том, как работают правила брандмауэра и что их составляет	Прежде чем изменять правила брандмауэра, необходимо изучить указанные ниже сведения о том, как они работают. ■ Как упорядочить правила, чтобы в начале проверялись самые строгие правила, а в конце — наиболее общие См. "Сведения о правилах и параметрах брандмауэра и порядке обработки при предотвращении вторжений" на стр. 92. ■ Клиент использует проверку с учетом состояния, благодаря которой отслеживается состояние сетевых подключений См. "Как брандмауэр использует проверку с учетом состояния" на стр. 93. ■ Компоненты брандмауэра, определяющие правило брандмауэра См. "Элементы правила брандмауэра на клиенте" на стр. 90.

Задача	Описание
Добавление нового правила брандмауэра	Для управления правилами брандмауэра можно выполнить следующие задачи. ■ Добавление собственных правил пользователя в правила, которые Symantec Endpoint Protection устанавливает по умолчанию См. "Добавление правил брандмауэра на клиенте" на стр. 94. ■ Настройка правила путем изменения какого-либо критерия правил брандмауэра ■ Экспорт и импорт правил брандмауэра из другой политики брандмауэра См. "Экспорт и импорт правил брандмауэра" на стр. 95. ■ Копирование и вставка правил брандмауэра

Элементы правила брандмауэра на клиенте

Когда один компьютер пытается подключиться к другому компьютеру, брандмауэр Symantec Endpoint Protection сравнивает тип соединения со списком правил брандмауэра. Для определения правил можно воспользоваться триггерами, в частности, приложениями, хостами или протоколами. Например, правило может связывать протокол с конкретным целевым адресом. Для того чтобы правило брандмауэра выполнилось, необходимо, чтобы сработали все триггеры. Если какой-то триггер для текущего пакета не сработал, правило не применяется.

Если пакет активирует какое-либо правило брандмауэра, брандмауэр не будет проверять другие правила. Если пакет не активирует никакого правила, брандмауэр автоматически блокирует этот пакет и не заносит это событие в журнал.

Правила брандмауэра задают условия, при которых сетевое соединение должно быть разрешено или заблокировано. Например, правило может разрешать трафик между удаленным портом 80 и IP-адресом 192.58.74.0 ежедневно с 9 утра до 5 вечера.

Табл. 4-3 описывает критерии, применяемые при создании правил брандмауэра.

Табл. 4-3 Критерии правил брандмауэра

Условие	Описание
Триггеры	■ Приложения Если приложение является единственным триггером в разрешающем трафик правиле, брандмауэр разрешит приложению выполнять любые сетевые операции. Важным показателем здесь является приложение, а не сетевые операции, которые это приложение выполняет. Допустим, что правилом разрешена программа Internet Explorer, а другие триггеры не определены. Пользователи смогут обращаться к удаленным сайтам по протоколам HTTP, HTTPS, FTP, Gopher и любым другим протоколам, поддерживаемым веб-браузером. Можно указать дополнительные триггеры, описывающие конкретные сетевые протоколы и хосты, подключение к которым разрешено. ■ Хосты Локальным хостом всегда является локальный клиентский компьютер, а удаленным хостом всегда является удаленный компьютер, расположенный где-либо в сети. Это выражение взаимосвязи хостов не зависит от направления трафика. Указывая хост в качестве триггера, пользователь всегда указывает удаленный хост, то есть противоположный конец сетевого соединения. ■ Протоколы Триггер протокола указывает один или несколько сетевых протоколов, использование которых нужно учитывать для описанного трафика. Локальный порт всегда принадлежит локальному хосту, а удаленный порт всегда принадлежит удаленному компьютеру. Это выражение взаимосвязи портов не зависит от направления трафика. ■ Сетевые адаптеры Если в качестве триггера указан сетевой адаптер, правило будет применяться только к трафику, проходящему через указанный тип адаптера в любом направлении. Можно указать любой адаптер или адаптер, связанный с клиентским компьютером. Критерии триггеров можно объединять для формирования более сложных правил — например, для идентификации конкретного протокола относительно определенного целевого адреса. Для того чтобы правило применялось, необходимо, чтобы сработали все триггеры. Если хотя бы один триггер для текущего пакета не срабатывает, брандмауэр не применяет правило.
Условия	■ Расписание и состояние заставки Параметры условий не описывают аспект сетевого соединения. Вместо этого условные параметры определяют активное состояние правила. Условные параметры не являются обязательными, и их можно не определять. Можно настроить расписание или указать состояние экранной заставки, которое определяет, является ли правило активным или неактивным. Неактивные правила не учитываются брандмауэром при получении пакетов.

Условие	Описание
Действия	■ Разрешить или заблокировать, заносить в журнал или не заносить в журнал Параметры действий указывают, какие действия должен предпринять брандмауэр, если правило сработало. Если правило было выбрано в результате получения пакета, то брандмауэр выполнит все действия. Брандмауэр разрешит или заблокирует пакет, а также занесет сведения об операции в журнал либо не будет этого делать. Если брандмауэр разрешает трафик, выбранному правилом трафику будет разрешен доступ к сети. Если брандмауэр блокирует трафик, выбранному правилом трафику будет запрещен доступ к сети.

См. "Как брандмауэр использует проверку с учетом состояния" на стр. 93.

См. "Добавление правил брандмауэра на клиенте" на стр. 94.

См. "Управление правилами брандмауэра" на стр. 89.

Сведения о правилах и параметрах брандмауэра и порядке обработки при предотвращении вторжений

Правила брандмауэра обрабатываются последовательно, от высшего к низшему приоритету в списке правил. Если первое правило не описывает способ обработки пакета, то брандмауэр проверяет второе правило. Обработка правил продолжается до обнаружения первого совпадения. После обнаружения подходящего правила брандмауэр выполняет указанное в нем действие. Все последующие правила с более низким приоритетом игнорируются. Например, если в начале списка указано правило, блокирующее весь трафик, за которым следует правило, разрешающее весь трафик, то клиент блокирует весь трафик.

Правила можно упорядочить в соответствии с уровнем конкретности. В этом случае первыми проверяются наиболее строгие, а в конце — наиболее общие правила. Например, правила, блокирующие трафик, должны быть расположены в верхней части списка правил. Правила, расположенные ниже, могут разрешать трафик.

Лучше всего при создании базового списка правил придерживаться следующего порядка.

1 Правила, блокирующие весь трафик.

2 Правила, разрешающие весь трафик.

3 Правила, разрешающие или блокирующие данные от конкретных компьютеров.

4 Правила, разрешающие или блокирующие данные от конкретных приложений, сетевых служб или через конкретные порты.

Табл. 4-4 описывает порядок обработки правил, настроек брандмауэра и предотвращения вторжений.

Табл. 4-4 Порядок обработки

Приоритет	Параметр
1	Пользовательские сигнатуры IPS
2	Параметры системы предотвращения вторжений, трафика и скрытого режима
3	Встроенные правила
4	Правила брандмауэра
5	Обнаружение сканирования портов
6	Сигнатуры IPS, загруженные с помощью LiveUpdate

См. "Принципы работы брандмауэра" на стр. 88.

Как брандмауэр использует проверку с учетом состояния

Для отслеживания текущих соединений брандмауэр использует функцию проверки с учетом состояния. Функция проверки с учетом состояния отслеживает исходные и целевые IP-адреса, порты, приложения и другую информацию о соединении. Перед обработкой правил брандмауэра клиент принимает решения относительно передачи трафика с учетом информации о соединении.

Например, если правило брандмауэра разрешает компьютеру подключаться к веб-серверу, то брандмауэр сохранит информацию о таком соединении. Получив ответ сервера, брандмауэр обнаружит, что ответ веб-сервера компьютеру ожидается. Он разрешит трафик веб-сервера в ответ на исходный запрос компьютера без проверки базы правила. Сохраняется информация только о тех исходящих соединениях, которые разрешены правилами.

Проверка с учетом состояния устраняет необходимость в создании новых правил. Если трафик передается в одном направлении, то не требуется создавать правила, разрешающие трафик в обоих направлениях. К трафику клиента, передаваемому в одном направлении, относятся Telnet (порт 23), HTTP (порт 80) и HTTPS (порт 443). Клиенты отправляют этот исходящий трафик; требуется создать правило, разрешающее исходящий трафик для указанных протоколов. Функция проверки с учетом состояния автоматически разрешит обратный трафик в ответ на исходящий трафик. Поскольку принцип действия брандмауэра основан на учете состояния, необходимо создать только правила, устанавливающие соединение, а не характеристики конкретных пакетов. Все пакеты, принадлежащие разрешенному соединению, разрешены явным образом как его составляющие.

Проверка с учетом состояния выполняется для всех правил, управляющих передачей данных TCP.

Однако такая проверка не выполняется для правил, фильтрующих данные ICMP. Для трафика ICMP требуется создать правила, разрешающие его передачу в обоих направлениях. Например, если клиент будет применять команду ping и получать ответы, то необходимо создать правило, разрешающее передавать пакеты ICMP в обоих направлениях.

Таблица состояния с информацией о соединениях периодически может очищаться. Например, она очищается, когда обрабатывается обновление политики брандмауэра или перезапускаются службы Symantec Endpoint Protection.

См. "Принципы работы брандмауэра" на стр. 88.

См. "Управление правилами брандмауэра" на стр. 89.

Добавление правил брандмауэра на клиенте

При добавлении или изменении правила брандмауэра на клиенте Symantec Endpoint Protection необходимо решить, что именно должно делать правило. Например, можно разрешить весь трафик от определенного источника или заблокировать пакеты UDP с веб-сайта.

Созданные правила брандмауэра будут включены автоматически.

Примечание: Можно добавлять или изменять правила брандмауэра в неуправляемых клиентах, а если администратор предоставит права на управление клиентом, то и в управляемых клиентах.

Для добавления правила брандмауэра

1. На боковой панели клиента выберите **Состояние**.
2. В разделе **Предупреждение последствий использования эксплойтов сети и хоста** выберите **Параметры > Настроить правила брандмауэра**.
3. В диалоговом окне **Настроить правила брандмауэра** нажмите кнопку **Добавить**, чтобы открыть пустое правило.

   Примечание: В управляемых клиентах это действие запускает мастер создания правила. Ниже приведены сведения о том, как настроить пустое правило.

   ---

4. На вкладке **Общие** пустого правила введите имя правила, затем выберите **Блокировать этот трафик** или **Разрешить этот трафик**.

5 Чтобы указать триггеры для правила, выберите и настройте как нужно каждую из вкладок:

- **Общие**
- **Хосты**
- **Порты и протоколы**
- **Приложения**
- **Расписание**

Например, можно выбрать сетевые адаптеры и хосты, на которые распространяется данное правило, а также интервалы времени, в течение которых правило активно/неактивно или регистрируются пакеты.

Примечание: С осторожностью настраивайте параметры записи в журнал пакетов, так как данные пакетов могут иметь большой размер.

См. "Элементы правила брандмауэра на клиенте" на стр. 90.

6 Нажмите кнопку **ОК**.

Правила активируются автоматически. Чтобы брандмауэр учитывал правила, их необходимо включить.

7 С помощью стрелок вверх и вниз можно изменить порядок правил.

8 Нажмите кнопку **ОК**.

Экспорт и импорт правил брандмауэра

Правила можно использовать совместно с другим клиентом, чтобы их не пришлось создавать заново. Для этого правила необходимо экспортировать с одного компьютера и импортировать на другой. При импорте правила добавляются в конец списка правил. Импортированные правила не заменяют существующие, даже если импортированное правило совпадает с существующим.

Экспортированные и импортируемые правила хранятся в файлах .sar.

Экспорт правил брандмауэра

1 На боковой панели на клиентском компьютере выберите **Состояние**.

2 В разделе **Предупреждение последствий использования эксплойтов сети и хоста** выберите **Параметры > Настроить правила брандмауэра**.

3 В диалоговом окне **Настроить правила брандмауэра** выберите правила, которые необходимо экспортировать.

4 Щелкните правила правой кнопкой мыши и выберите команду **Экспортировать выбранные правила**.

5 В диалоговом окне **Экспорт** укажите имя файла, затем нажмите кнопку **Сохранить**.

6 Нажмите кнопку **ОК**.

Импорт правил брандмауэра

1 На боковой панели на клиентском компьютере выберите **Состояние**.

2 В разделе **Предупреждение последствий использования эксплойтов сети и хоста** выберите **Параметры > Настроить правила брандмауэра**.

3 В диалоговом окне **Настроить правила брандмауэра** щелкните правой кнопкой мыши список правил и выберите команду **Импортировать правило**.

4 В диалоговом окне **Импорт** найдите файл .sar, содержащий импортируемые правила.

5 Нажмите кнопку **Открыть**.

6 Нажмите кнопку **ОК**.

См. "Добавление правил брандмауэра на клиенте" на стр. 94.

Настройка параметров брандмауэра

Можно включить параметры брандмауэра клиента, чтобы защитить компьютер от сетевых атак определенных типов. Некоторые из параметров заменяют правила брандмауэра, которые надо было бы добавить.

Примечание: Возможно, что администратор ограничил ваш доступ к некоторым из этих параметров.

Табл. 4-5 описывает типы параметров брандмауэра, которые можно настроить для дополнительной защиты.

Табл. 4-5 Настройки брандмауэра

Категория	Описание
Встроенные правила для важных сетевых служб	Symantec Endpoint Protection предоставляет встроенные правила, разрешающие нормальный обмен данными некоторым важным сетевым службам. Встроенные правила позволяют устранить необходимость в создании правил брандмауэра, явно разрешающих эти службы. В ходе обработки эти правила анализируются до правил брандмауэра, поэтому любой пакет, прошедший обработку встроенным правилом, будет разрешен. Встроенные правила можно настроить для служб DHCP, DNS и WINS.

Категория	Описание
Трафик и скрытый режим просмотра веб-страниц	Чтобы защитить клиент от некоторых типов сетевых атак, можно включить различные параметры трафика и скрытого просмотра веб-страниц. Опции трафика настраиваются с целью обнаружения и блокирования попыток доступа с помощью драйверов, NetBIOS и Token Ring. Можно настроить параметры проверки трафика для выявления скрытых атак других типов. Также можно управлять обработкой IP-трафика, который не соответствует правилам брандмауэра.
Предоставление общего доступа к сетевым файлам и принтерам	В клиенте можно разрешить совместный доступ к его файлам или обращение к общим папкам и принтерам в локальной сети. Для предотвращения сетевых атак совместное использование файлов и принтеров можно отключить. См. "Активация совместного доступа к сетевым файлам и принтерам на компьютерах с уже установленным клиентом Symantec Endpoint Protection" на стр. 98.
Обнаружение и блокирование атак	Когда клиент Symantec Endpoint Protection обнаруживает атаку из сети, он может автоматически блокировать соединение, чтобы обеспечить безопасность клиентского компьютера. Затем клиент автоматически блокирует все входящие и исходящие соединения с IP-адресом атакующего компьютера на заданный период времени. IP-адрес атакующего компьютера блокируется для одного расположения.
Управление входящим трафиком	Можно настроить клиент так, чтобы он блокировал входящий и исходящий трафик в указанных ниже ситуациях. ■ Если на вашем компьютере активирована заставка. ■ Если не запущен брандмауэр. ■ В любое время, когда необходимо заблокировать входящий и исходящий трафик. См. "Блокирование трафика при включении экранной заставки или когда не запущен брандмауэр" на стр. 102.

Как настроить параметры брандмауэра

1. В окне клиента выберите пункт **Изменить параметры**.
2. В разделе **Предупреждение последствий использования эксплойтов сети и хоста** нажмите **Настроить параметры**.
3. На вкладке **Брандмауэр** выберите параметры, которые требуется включить.

   Щелкните **Справка** для получения дополнительных сведений о настройках.
4. Нажмите кнопку **ОК**.

См. "Управление правилами брандмауэра" на стр. 89.

См. "Добавление правил брандмауэра на клиенте" на стр. 94.

Активация совместного доступа к сетевым файлам и принтерам на компьютерах с уже установленным клиентом Symantec Endpoint Protection

В клиенте можно разрешить совместный доступ к его файлам или обращение к общим папкам и принтерам в локальной сети. Для предотвращения сетевых атак совместное использование файлов и принтеров можно отключить.

Табл. 4-6 Способы разрешения совместного доступа к сетевым папкам и принтерам

Задача	Описание
Автоматически разрешить совместный доступ к сетевым папкам и принтерам на вкладке **Сеть Microsoft Windows**.	Если в брандмауэре настроен запрет этого трафика, то правило брандмауэра считается более приоритетным, чем эти параметры. См. "Как автоматически разрешить совместный доступ к сетевым файлам и принтерам и просмотр сети" на стр. 98.
Вручную разрешить совместный доступ к сетевым папкам и принтерам, добавив правила брандмауэра.	Правила брандмауэра предоставляют более широкие возможности для настройки, чем стандартные параметры. Например, правило можно создать для одного хоста, а не для всех хостов. Правила брандмауэра разрешают доступ к портам, через которые можно просматривать файлы и принтеры и работать с ними. Один набор правил можно создать для предоставления совместного доступа к файлам клиента. Второй набор правил можно создать для предоставления клиенту доступа к папкам и принтерам других компьютеров. См. "Как вручную разрешить совместный доступ к сетевым файлам и принтерам и просмотр сети" на стр. 99. См. "Как вручную разрешить другим компьютерам просматривать файлы на клиентском компьютере" на стр. 99.

Как автоматически разрешить совместный доступ к сетевым файлам и принтерам и просмотр сети

1. На боковой панели клиента выберите **Состояние**.
2. В разделе **Предупреждение последствий использования эксплойтов сети и хоста** выберите **Параметры** > **Изменить параметры**.
3. На вкладке **Сеть Microsoft Windows** выберите один из следующих параметров.
   - Чтобы разрешить просмотр других компьютеров и принтеров в сети, включите переключатель **Показать папки и принтеры в сети**.

- Чтобы разрешить другим компьютерам просматривать файлы на вашем компьютере, включите переключатель **Разрешить общий доступ к моим папкам и принтерам в сети**.

4 Нажмите кнопку **ОК**.

Как вручную разрешить совместный доступ к сетевым файлам и принтерам и просмотр сети

1 На боковой панели клиента выберите **Состояние**.

2 В разделе **Предупреждение последствий использования эксплойтов сети и хоста** выберите **Параметры** > **Изменить параметры** > **Настроить правила брандмауэра**.

Примечание: Этот параметр доступен в том случае, если администратор предоставил вам доступ, либо в случае использования неуправляемого клиента.

---

3 В диалоговом окне **Настроить правила брандмауэра** нажмите кнопку **Добавить**.

4 На вкладке **Общие** введите имя правила и выберите **Разрешить этот трафик**.

5 На вкладке **Порты и протоколы** в выпадающем списке **Протокол** выберите **TCP**.

6 В раскрывающемся списке **Удаленные порты** введите следующее:

88, 135, 139, 445

7 Нажмите кнопку **ОК**.

8 В диалоговом окне **Настроить правила брандмауэра** нажмите кнопку **Добавить**.

9 На вкладке **Общие** введите имя правила и выберите **Разрешить этот трафик**.

10 На вкладке **Порты и протоколы** в выпадающем списке **Протокол** выберите **UDP**.

11 В раскрывающемся списке **Удаленные порты** введите следующее:

88

12 В раскрывающемся списке **Локальные порты** введите следующее:

137, 138

13 Нажмите кнопку **ОК**.

Как вручную разрешить другим компьютерам просматривать файлы на клиентском компьютере

1 На боковой панели клиента выберите **Состояние**.

2 В разделе **Предупреждение последствий использования эксплойтов сети и хоста** нажмите **Настроить параметры**.

3 В диалоговом окне **Настроить правила брандмауэра** нажмите кнопку **Добавить**.

4 На вкладке **Общие** введите имя правила и выберите **Разрешить этот трафик**.

5 На вкладке **Порты и протоколы** в выпадающем списке **Протокол** выберите **TCP**.

6 В раскрывающемся списке **Локальные порты** введите следующее:

88, 135, 139, 445

7 Нажмите кнопку **ОК**.

8 В диалоговом окне **Настроить правила брандмауэра** нажмите кнопку **Добавить**.

9 На вкладке **Общие** введите имя правила и выберите **Разрешить этот трафик**.

10 На вкладке **Порты и протоколы** в выпадающем списке **Протокол** выберите **UDP**.

11 В раскрывающемся списке **Локальные порты** введите следующее:

88, 137, 138

12 Нажмите кнопку **ОК**.

См. "Настройка параметров брандмауэра" на стр. 96.

Разрешение и блокировка доступа приложений к сети

Можно настроить Symantec Endpoint Protection так, чтобы он разрешал или блокировал доступ к сети для приложения или чтобы запрашивал пользователя о необходимом действии. В результате этого действия будет создано правило брандмауэра, указывающее, может ли приложение, работающее на вашем компьютере, получить доступ к сети. Такие правила называются правилами брандмауэра для приложений.Например, можно заблокировать доступ к любым веб-сайтам для браузера Internet Explorer, работающего на вашем компьютере.

Табл. 4-7 Действия брандмауэра при обращении приложений к клиенту или к сети

Действие	Описание
Разрешить	Разрешает входящему трафику получить доступ к клиентскому компьютеру, а исходящему трафику — доступ к сети. Если клиент получает трафик, в левом нижнем углу значка отображается небольшая синяя точка. Если клиент отправляет трафик, точка отображается в правом нижнем углу значка.
Блокировать	Блокирует входящему и исходящему трафику доступ к сети или подключению к Интернету.

Действие	Описание
Спросить	Запрашивает, следует ли разрешить приложению доступ к сети при следующем запуске.
Прервать	Останавливает процесс.

Как разрешить или заблокировать приложению доступ к сети

1. На боковой панели клиента выберите **Состояние**.
2. В разделе **Предупреждение последствий использования эксплойтов сети и хоста** выберите **Параметры > Показать сетевые операции**.
3. В диалоговом окне **Сетевые операции** щелкните правой кнопкой мыши работающее приложение или службу, а затем выберите действие, которое клиент должен выполнить для этого приложения.

   Если выбрать один из пунктов **Разрешить**, **Блокировать** или **Спрашивать**, будет создано правило брандмауэра только для этого приложения.

   См. "Разрешение и блокировка приложений, которые уже запущены на клиенте" на стр. 101.
4. Нажмите кнопку **Закрыть**.

Разрешение и блокировка приложений, которые уже запущены на клиенте

Можно настроить условия разрешения и блокировки приложений, которые уже запущены на клиентском компьютере. Например, для видеоигры можно разрешить доступ в сеть только в определенные часы. Правила брандмауэра для приложений также называются параметрами приложений.

См. "Разрешение и блокировка доступа приложений к сети" на стр. 100.

Примечание: Если правило брандмауэра для приложения противоречит правилу брандмауэра, то правило брандмауэра считается более приоритетным. Например, правило брандмауэра, блокирующее весь трафик с 1:00 до 8:00, имеет приоритет перед правилом брандмауэра для приложения, позволяющим запуск iexplore.exe в любое время.

Как разрешить или заблокировать приложения, которые уже запущены на клиенте

1. На боковой панели клиента выберите **Состояние**.
2. В разделе **Предупреждение последствий использования эксплойтов сети и хоста** выберите **Параметры > Показать параметры приложений**.
3. В диалоговом окне **Показать параметры приложений** можно изменить действие, щелкнув приложение правой кнопкой и выбрав **Разрешить**, **Спросить** или **Блокировать**.
4. Чтобы изменить другие параметры правила для приложения, щелкните **Настроить**.
5. В диалоговом окне **Настроить параметры приложения** настройте ограничения или исключения для выбранного приложения.

   Если на шаге 3 задано действие **Разрешить**, любые настроенные параметры являются ограничениями правила. Если задано действие **Блокировать**, настроенные параметры являются исключениями из правила.

   Для просмотра дополнительных сведений об этих параметрах щелкните **Справка**.
6. Чтобы принять изменения конфигурации, нажмите кнопку **ОК**.
7. Чтобы удалить правило, заданное для приложения, щелкните имя приложения и нажмите кнопку **Удалить**. При удалении ограничений также удаляется и действие, предпринимаемое клиентом по отношению к приложению. При следующем подключении приложения или службы к сети может снова появиться вопрос о том, следует ли разрешить или заблокировать соединение.

   Чтобы удалить все правила брандмауэра для приложений, щелкните **Удалить все**.
8. Нажмите кнопку **ОК**, чтобы закрыть диалоговое окно **Показать параметры приложений**.

См. "Добавление правил брандмауэра на клиенте" на стр. 94.

Блокирование трафика при включении экранной заставки или когда не запущен брандмауэр

На компьютере можно настроить блокирование входящего и исходящего трафика в следующих ситуациях.

Если включается экранная заставка компьютера	Компьютер может блокировать весь входящий и исходящий сетевой трафик, когда включена экранная заставка. При выключении заставки компьютер возвращается на предыдущий уровень безопасности. См. "Как блокировать трафик при включении экранной заставки" на стр. 103.

Если не запущен брандмауэр	Компьютер не защищен с момента включения компьютера до момента запуска службы брандмауэра, а также с момента выключения службы брандмауэра до момента выключения компьютера. В эти отрезки времени безопасность не обеспечивается, и возможен несанкционированный обмен данными. См. "Блокирование трафика на время, когда не запущен брандмауэр" на стр. 103.
В любое время, когда необходимо заблокировать входящий и исходящий трафик	Сетевой трафик можно заблокировать при обнаружении особенно разрушительных вирусных атак на сеть или подсеть компании. В обычных условиях делать это не требуется. **Примечание:** Обратите внимание, что администратор мог блокировать этот параметр. В неуправляемом клиенте блокировать весь трафик нельзя. См. "Блокирование сетевого трафика в любое время" на стр. 104.

Выключив защиту от сетевых угроз, можно разрешить весь трафик.

См. "Включение защиты на клиентском компьютере" на стр. 114.

Как блокировать трафик при включении экранной заставки

1. На боковой панели клиента нажмите **Изменить параметры**.
2. В разделе **Предупреждение последствий использования эксплойтов сети и хоста** нажмите **Настроить параметры**.
3. На вкладке **Сеть Microsoft Windows** выберите **Блокировать трафик сети Microsoft Windows во время работы экранной заставки**.
4. Нажмите кнопку **ОК**.

Блокирование трафика на время, когда не запущен брандмауэр

1. На боковой панели клиента нажмите **Изменить параметры**.
2. В разделе **Предупреждение последствий использования эксплойтов сети и хоста** нажмите **Настроить параметры**.
3. На вкладке **Брандмауэр** в разделе **Параметры трафика** выберите **Блокировать весь трафик, когда брандмауэр не работает**.

   Если отключить параметр **Разрешить начальный трафик DHCP и NetBIOS**, начальный трафик, который обеспечивает подключение к сети, будет блокироваться.
4. Нажмите кнопку **ОК**.

Блокирование сетевого трафика в любое время

1. На боковой панели клиента выберите **Состояние**.
2. В разделе **Предупреждение последствий использования эксплойтов сети и хоста** выберите **Параметры > Показать сетевые операции**.
3. Выберите **Сервис > Блокировать весь трафик**.
4. Для подтверждения нажмите **Да**.
5. Для возврата к прежним значениям параметров брандмауэра выключите переключатель **Сервис > Блокировать весь трафик**.

См. "Настройка параметров брандмауэра" на стр. 96.

Настройка предотвращения вторжений

По умолчанию компонент предотвращения вторжений работает на компьютере постоянно. Предотвращение вторжений перехватывает данные на сетевом уровне. Для сканирования пакетов или их потоков оно использует сигнатуры. Каждый пакет сканируется индивидуально и сверяется с шаблонами, соответствующими атакам на сеть или браузер. Предотвращение вторжений — это второй после брандмауэра уровень защиты клиентских компьютеров. Функцию предотвращения вторжений иногда называют системой предотвращения вторжений (IPS).

Примечание: Предотвращение вторжений и брандмауэр — это компоненты системы защиты от сетевых угроз. Система предупреждения последствий использования эксплойтов сети и хоста включает в себя компоненты "Защита от сетевых угроз" и "Предупреждение последствий использования эксплойтов памяти".

Как управлять функцией предотвращение вторжений:

1. Убедитесь, что загружены самые актуальные сигнатуры IPS.

   По умолчанию в клиент загружаются самые актуальные сигнатуры. Однако загрузку сигнатур можно выполнить вручную немедленно.

   См. "Обновление содержимого клиента с помощью LiveUpdate" на стр. 20.

2. Не отключайте систему предотвращения вторжений.

   Она должна работать постоянно. Symantec Endpoint Protection регистрирует попытки и события вторжения в журнале безопасности. Symantec Endpoint Protection может регистрировать события вторжения и в журнале пакетов, если администратор настроил соответствующие параметры.

   См. "Просмотр журналов" на стр. 119.

См. "Включение журнала пакетов" на стр. 119.

3. Если вам кажется, что обнаруженный файл ошибочно считается угрозой, сообщите об этом администратору.

   Непредвиденные события необязательно являются ложным срабатыванием.

   Рекомендации по обработке ошибочных положительных обнаружений IPS в Symantec Endpoint Protection

---

Примечание: Обратите внимание, что администратор мог блокировать эти параметры.

Включение функции предотвращения вторжений

Система предотвращения вторжений включает в себя два типа:

- Система предотвращения вторжений для сети
  Для идентификации атак на клиентские компьютеры система предотвращения вторжений для сети использует сигнатуры. Для известных атак система предотвращения вторжений автоматически отбрасывает пакеты, соответствующие сигнатурам.
- Система предотвращения вторжений для браузера
  Предотвращение вторжений в браузер отслеживает атаки на браузеры Internet Explorer и Firefox. Браузеры всех других типов не поддерживают систему предотвращения вторжений для браузера. Последние сведения о браузерах, которые защищает система предотвращения вторжений, см. в статье: Поддерживаемые версии браузеров для системы предотвращения вторжений для браузера.

При обнаружении атаки из сети клиент может показывать уведомление.

См. раздел: Как включить уведомления системы предотвращения вторжений

Как включить функцию предотвращения вторжений

1 На боковой панели клиента нажмите **Изменить параметры**.

2 В разделе **Предупреждение последствий использования эксплойтов сети и хоста** нажмите **Настроить параметры**.

3 Убедитесь, что на вкладке **Предотвращение вторжений** установлены следующие флажки:

   - **Включить систему предотвращения вторжений для сети**
   - **Включить систему предотвращения вторжений для браузера**
     Также можно настроить функцию предотвращения вторжений для браузера так, чтобы обнаружения только регистрировались в журнале, но не блокировались. Эту конфигурацию следует использовать лишь временно, так как она понижает уровень защиты компьютера. Например, режим только регистрации можно

включить на время устранения проблем с блокированием трафика. После просмотра журнала безопасности и обнаружения и исключения сигнатур, блокирующих трафик, режим только регистрации можно выключить.

4 Нажмите кнопку **ОК**.

Как включить уведомления системы предотвращения вторжений

1 На боковой панели клиента нажмите **Изменить параметры**.

2 В разделе "Предупреждение последствий использования эксплойтов сети и хоста" нажмите **Настроить параметры**.

3 Убедитесь, что на вкладке **Уведомления** установлен флажок **Показать уведомления о предотвращении вторжений и предупреждении последствий использования эксплойтов памяти**.

4 Нажмите кнопку **ОК**.

Предотвращение атак на уязвимые приложения

Предупреждение последствий использования эксплойтов памяти (MEM) блокирует атаки на часто используемые приложения, выполняемые на компьютере Windows. При обнаружении попытки использования эксплойта клиент выводит одно из следующих сообщений (или оба).

- `Symantec Endpoint Protection: Атака: обнаружено событие перезаписи структурного обработчика исключений`

  Клиент блокирует эксплойт без прерывания работы приложения.

- `Symantec Endpoint Protection завершит работу приложения`

  Клиент завершает работу приложения.

Если работа приложения часто прерывается, выполните следующие действия:

1. Поставьте в известность администратора.
2. Определите, действительно ли приложение находится под угрозой или произошло ложное срабатывание.
   - Если приложение действительно является объектом атаки, проверьте, установлены ли связанные исправления или новый выпуск, в котором текущая уязвимость исправлена. После установки исправления заново запустите приложение на клиентском компьютере, чтобы проверить наличие угрозы.
   - В случае ложного срабатывания временно отключите предупреждение последствий использования эксплойтов памяти. Поставьте в известность администратора или группу Symantec Security Response. Не включайте предупреждение последствий использования эксплойтов памяти, пока проблема

не будет устранена компанией Symantec. Затем снова включите предупреждение последствий использования эксплойтов памяти.

Как определить, что произошло ложное срабатывание

1 С помощью журнала безопасности убедитесь, что работа приложения была прервана компонентом Предупреждение последствий использования эксплойтов памяти.

Например, может быть показано следующее событие: `Attack: Blocked Structured Exception Handler Overwrite attack against C:\Program Files (x86)\Adobe\Reader 9.0\Reader\AcroRd32.exe`

См. "Просмотр журналов" на стр. 119.

2 Выключить предупреждение последствий использования эксплойтов памяти.

3 Повторно запустите приложение.

- Правильная работа приложения будет свидетельствовать о ложном срабатывании.
- В случае необычных действия приложения (например, запуск другого приложения) обнаруженная угроза является истинной.

Администратор может запретить отключение предупреждения последствий использования эксплойтов памяти для управляемых клиентов.

Как отключить и заново включить предупреждение последствий использования эксплойтов памяти

1 На странице **Состояние** рядом с разделом **Предупреждение последствий использования эксплойтов сети и хоста** выберите **Параметры**.

2 Выберите одну из следующих задач в раскрывающемся меню:

- Нажмите **Выключить предупреждение последствий использования эксплойтов памяти** или **Включить предупреждение последствий использования эксплойтов памяти**.
- Откройте вкладку **Изменить параметры** > **Предупреждение последствий использования эксплойтов памяти** и установите/снимите флажок **Включить предупреждение последствий использования эксплойтов памяти**.

Глава 5

Управление клиентом

В этой главе рассмотрены следующие вопросы:

- Управление клиентом
- Обновление политик клиента
- Сведения об управляемых и неуправляемых клиентах
- Проверка типа клиента — управляемый или неуправляемый
- Скрытие и отображение значка в области уведомлений на клиенте Symantec Endpoint Protection
- Включение защиты на клиентском компьютере

Управление клиентом

По умолчанию клиентский компьютер защищен, и дополнительная настройка клиента не требуется. Но бывают такие ситуации, когда требуется изменить защиту:

- На компьютере выполняется неуправляемый клиент.
  После установки неуправляемого клиента управлять защитой компьютера может только сам пользователь. Неуправляемый клиент защищен по умолчанию, но пользователю может понадобиться изменить настройки защиты компьютера.
  См. "Сведения об управляемых и неуправляемых клиентах" на стр. 111.
  См. "Проверка типа клиента — управляемый или неуправляемый" на стр. 113.
- Требуется включить или выключить некоторые технологии защиты.
  См. "Включение защиты на клиентском компьютере" на стр. 114.
- Требуется проверить наличие последних описаний вирусов и содержимого безопасности в системе.
- Появились сведения о новом вирусе или угрозе безопасности, и требуется выполнить сканирование.

Табл. 5-1 Задачи по настройке клиента

Шаг	Описание
Реакция на предупреждения и уведомления	Правильно реагируйте на сообщения, требующие ввода данных. Например, в процессе сканирования может быть обнаружен вирус или угроза безопасности. Тогда появятся результаты сканирования с запросом, что следует сделать. См. "Типы предупреждений и уведомлений" на стр. 23.
Проверка состояния защиты	Пользователю следует регулярно проверять страницу **Состояние**, чтобы удостовериться, что все типы защиты включены и работают. См. "Включение защиты на клиентском компьютере" на стр. 114. См. "значки состояния клиента Symantec Endpoint Protection" на стр. 16.
Обновление описаний вирусов и содержимого безопасности	Следует проверять, имеются ли на компьютере самые последние описания вирусов и содержимое безопасности. ■ Убедитесь, что в системе установлены последние обновления функций защиты. Даты и номера этих файлов можно проверить на странице **Состояние** клиента под каждым типом защиты. ■ Получите последние обновления защиты. См. "Обновление содержимого клиента с помощью LiveUpdate" на стр. 20. Пользователь может выполнять эти задачи на управляемом клиенте, если это разрешено администратором.
Просканируйте свой компьютер	Запустите сканирование, чтобы убедиться, что на компьютере или в почтовых приложениях нет вирусов. По умолчанию клиент сканирует компьютер при включении, но также сканирование можно выполнить в любое другое время. См. "Немедленное сканирование клиентского компьютера" на стр. 18.
Регулировка параметров защиты	В большинстве случаев значения параметров по умолчанию обеспечивают нормальную защиту компьютера. Но при необходимости можно повысить или понизить степень защиты следующим образом: ■ Планировать дополнительные сканирования См. "Управление сканированием на локальном компьютере" на стр. 35. ■ Добавлять правила брандмауэра (только на неуправляемом клиенте) См. "Управление защитой с помощью брандмауэра" на стр. 87.

Шаг	Описание
Проверка соответствия требованиям	Проверьте, соответствует ли компьютер требованиям политики безопасности компании. См. "Проверка соблюдения требований безопасности с помощью сканирования целостности хоста" на стр. 83.
Просмотр журналов на наличие угроз или атак	Проверьте по журналу, предпринимались ли сетевые атаки на клиент, и выясните, заражен ли он вирусами. См. "Просмотр журналов" на стр. 119.
Обновление политики безопасности (Только управляемый клиент)	Убедитесь, что клиент получил последнюю политику безопасности с сервера управления. Политика безопасности содержит последние параметры для технологий защиты клиента. См. "значки состояния клиента Symantec Endpoint Protection" на стр. 16. Обновление политики безопасности осуществляется автоматически. Тем не менее можно обновить ее вручную, чтобы гарантировать наличие самой новой версии. См. "Обновление политик клиента" на стр. 110.

Обновление политик клиента

Если есть сомнение, что на клиенте установлена самая новая политика, то политики на клиентском компьютере Symantec Endpoint Protection можно обновить вручную. Если клиент не получает обновления, это может быть вызвано нарушением связи.

Проверьте серийный номер политики, чтобы убедиться, что управляемые клиентские компьютеры имеют связь с сервером управления.

Политику на клиентском компьютере можно обновить только вручную. Если политикой вам запрещено открывать пользовательский интерфейс клиента или значок в области уведомлений, обновление политики вручную невозможно.

Как обновить политику клиента из Symantec Endpoint Protection Manager

1. В консоли выберите пункт **Клиенты**.
2. Щелкните правой кнопкой мыши группу клиентов, для которых необходимо обновить политику, и выберите **Выполнить команду для группы > Обновить содержимое**.
3. Нажмите кнопку **Да**, а затем — кнопку **ОК**.

Как обновить политику клиента с помощью панели задач Windows

1. В области уведомлений на панели задач Windows щелкните правой кнопкой значок Symantec Endpoint Protection.
2. Выберите **Обновить политику**.

Как обновить политику клиента с помощью пользовательского интерфейса клиента

1. В клиенте выберите пункт **Справка > Устранение неполадок**.
2. В левом столбце окна **Устранение неполадок** выберите **Управление**.
3. На панели **Управление** в разделе **Профиль политики** выберите один из следующих вариантов.
   - Нажмите кнопку **Обновить**, чтобы обновить политику напрямую из консоли управления.
   - Нажмите кнопку **Импортировать**, чтобы импортировать политику, экспортированную из консоли управления. В ответ на приглашение выберите файл политики для импорта.

Сведения об управляемых и неуправляемых клиентах

Администратор может установить клиент как управляемый (установкой управляет администратор) или неуправляемый (автономная установка).

Табл. 5-2 Различия между управляемым и неуправляемым клиентом

Тип клиента	Описание
Управляемый клиент	Управляемый клиент обменивается данными с сервером управления, находящимся в той же сети. Администратор настраивает защиту и параметры по умолчанию. Сервер управления уведомляет клиента, и клиент загружает настройки. В зависимости от настроек связи сервера управления, если администратор вносит изменение в параметры защиты, клиент практически немедленно загружает это изменение. Администратор может изменить уровень взаимодействия пользователя с клиентом следующими способами. ■ Администратор полностью управляет клиентом. При этом пользователь вообще не вмешивается в настройку. Все параметры заблокированы или недоступны, но пользователь может просматривать информацию о работе клиента на своем компьютере. ■ Клиент управляется администратором, но пользователь может изменять некоторые параметры клиента и выполнять некоторые задачи. Например, пользователю может быть разрешено запускать свои сеансы сканирования и вручную загружать обновления клиента и защиты. ■ Клиент управляется администратором, но пользователь может изменять все параметры клиента и выполнять все задачи, связанные с защитой. Доступность параметров клиента и набор значений, которые могут принимать эти параметры, может периодически изменяться. Например, параметр может измениться после того, как администратор обновит политику, управляющую защитой клиента.
Неуправляемые клиенты	Неуправляемый клиент не обменивается данными с сервером управления и не управляется администратором. Тип неуправляемого клиента может быть одним из перечисленных ниже. ■ Автономный компьютер, не подключенный к сети, например домашний или портативный компьютер. На компьютере должен быть установлен клиент Symantec Endpoint Protection с параметрами по умолчанию или параметрами, заранее заданными администратором. ■ Удаленный компьютер, применяемый для подключения к корпоративной сети. Подключение будет разрешено, если компьютер соответствует требованиям к безопасности. Однако на неуправляемых клиентах целостность хоста не поддерживается. При первой установке клиент использует значения по умолчанию. После установки пользователь может изменять любые параметры и выполнять любые задачи защиты.

Табл. 5-3 описывает различия в пользовательском интерфейсе между управляемым и неуправляемым клиентами.

Табл. 5-3 Различия между управляемым и неуправляемым клиентом с учетом области функций

Область функций	Централизованно управляемый клиент	Неуправляемый клиент
Защита от вирусов и программ-шпионов	Для параметров, недоступных для настройки, отображается значок в виде закрытого замка, а сами параметры показаны серым цветом.	Ни закрытый, ни открытый замки в клиенте не отображаются.
Превентивная защита от угроз	Для параметров, недоступных для настройки, отображается значок в виде закрытого замка, а сами параметры показаны серым цветом.	Клиент не показывает ни закрытый замок, ни открытый замок.
Управление клиентом и параметры предупреждения последствий использования эксплойтов сети и хоста	Параметры, управляемые администратором, не отображаются.	Отображаются все параметры.

См. "Проверка типа клиента — управляемый или неуправляемый" на стр. 113.

Проверка типа клиента — управляемый или неуправляемый

Чтобы выяснить, в каком объеме пользователь может управлять защитой клиента, необходимо сначала определить тип клиента: управляемый или неуправляемый. На неуправляемом клиенте можно настроить больше параметров, чем на управляемом клиенте.

См. "Сведения об управляемых и неуправляемых клиентах" на стр. 111.

Проверка типа клиента — управляемый или неуправляемый

1. На странице **Состояние** выберите **Справка > Устранение неполадок**.
2. В окне **Устранение неполадок** выберите **Управление**.
3. На панели **Управление** в разделе **Общая информация** посмотрите значение поля **Сервер**.
   - Если клиент управляемый, то в поле **Сервер** будет отображаться либо адрес сервера управления, либо текст **Отключен**.

Адрес может представлять собой IP-адрес, имя DNS или имя NetBIOS. Например, в поле может стоять имя DNS "SEPMServer1". Если клиент управляемый, но в данный момент не подключен к серверу управления, в поле будет отображаться текст **Отключен**.

- Для неуправляемого клиента в поле **Сервер** будет указано значение **Автономное управление**.

4 Нажмите кнопку **Закрыть**.

Скрытие и отображение значка в области уведомлений на клиенте Symantec Endpoint Protection

При необходимости можно скрыть значок Symantec Endpoint Protection в области уведомлений (иногда его называют значком панели задач). Например, это можно сделать, если в панели задач Windows недостаточно места.

См. "значки состояния клиента Symantec Endpoint Protection" на стр. 16.

Как скрыть или отобразить значок в области уведомлений на клиенте

Примечание: В управляемых клиентах значок в области уведомлений нельзя скрыть, если это запрещено администратором.

---

1 В окне клиента выберите пункт **Изменить параметры**.

2 На странице **Изменить параметры** нажмите **Настроить параметры** рядом с пунктом **Управление клиентами**.

3 В окне **Параметры управления клиентами** на вкладке **Общие** в разделе **Параметры отображения** установите или снимите отметку переключателя **Показывать значок защиты Symantec в области уведомления**.

4 Нажмите кнопку **ОК**.

Включение защиты на клиентском компьютере

На компьютере должны постоянно работать все виды защиты, особенно функция автоматической защиты.

Клиент, в котором выключены некоторые виды защиты

- Строка состояния наверху страницы **Состояние** имеет красный цвет.

- Значок клиента отображается в виде универсального символа запрета - перечеркнутый красный круг. Значок клиента выглядит как щит на панели задач в правом нижнем углу рабочего стола Windows. В некоторых конфигурациях значок не отображается.
  См. "значки состояния клиента Symantec Endpoint Protection" на стр. 16.

В управляемом клиенте администратор может включать и отключать любую технологию защиты в любое время. Если пользователь отключил защиту, администратор может в дальнейшем снова включить ее. Администратор также может заблокировать защиту, чтобы пользователь не мог ее отключить.

Как включить технологии защиты с помощью страницы "Состояние"

- В клиенте, в верхней части страницы **Состояние** выберите **Исправить** или **Исправить все**.

Как включить технологии защиты с помощью панели задач

- В области уведомлений рабочего стола Windows щелкните правой кнопкой значок клиента и выберите **Включить Symantec Endpoint Protection**.

Как включить технологии защиты на клиентском компьютере

- На странице **Состояние** клиента в разделе **Защита *<тип защиты>*** выберите **Параметры > Включить защиту *<тип защиты>***.

Как включить брандмауэр

1. В верхней части страницы **Состояние** клиента рядом с разделом **Предупреждение последствий использования эксплойтов сети и хоста** выберите **Параметры** > **Изменить параметры**.
2. На вкладке **Брандмауэр** установите флажок **Включить брандмауэр**.
3. Нажмите кнопку **ОК**.

См. "Включение автоматической защиты" на стр. 74.

Глава 6

Устранение неполадок клиента

В этой главе рассмотрены следующие вопросы:

- Устранение неполадок на компьютере с помощью средства Symantec Diagnostic Tool (SymDiag)
- Сведения о журналах
- Просмотр журналов

Устранение неполадок на компьютере с помощью средства Symantec Diagnostic Tool (SymDiag)

Это средство можно загрузить для диагностики распространенных неполадок, возникающих при установке и использовании клиента Symantec Endpoint Protection.

Средство поддержки помогает в решении следующих проблем.

- Позволяет быстро и точно определить известные проблемы.
- Когда средство распознает проблему, оно перенаправляет пользователя на ресурсы, позволяющие ему самостоятельно устранить эту проблему.
- Если проблема не устранена, средство позволяет с легкостью отправить данные в службу поддержки для дальнейшей диагностики.

Как устранить неполадки на компьютере с помощью средства Symantec Diagnostic Tool (SymDiag)

1 Выполните одно из следующих действий:

- См.: Загрузка Symantec Diagnostic Tool (SymDiag) для обнаружения неполадок в продуктах Symantec

- В Symantec Endpoint Protection Manager или клиенте нажмите **Справка > Загрузить Symantec Diagnostic Tool**

2 Следуйте инструкциям на экране.

Сведения о журналах

В журналах содержится информация об изменениях конфигурации клиента, о связанных с защитой операциях, а также об ошибках. Эти записи называются событиями.

Сведения о связанных с защитой операциях могут включать информацию об обнаружении вирусов, о состоянии компьютера, а также о входящем и исходящем трафике. Журналы управляемого клиента можно регулярно передавать на сервер управления. Используя эти данные, администратор может анализировать общее состояние безопасности сети.

Журналы являются важным инструментом для контроля над операциями локального компьютера и его взаимодействием с другими компьютерами и сетями. Используя информацию из журналов, можно определять общие тенденции распространения вирусов, угроз и атак на компьютер.

Для получения дополнительной информации о журнале нажмите F1, чтобы просмотреть справку по журналу.

Табл. 6-1 Журналы клиента

Журнал	Описание
Журнал управления	Содержит информацию об обращениях приложения к разделам реестра Windows, библиотекам DLL и файлам, а также о запущенных на компьютере приложениях.
Журнал отладки	Содержат информацию о клиенте, сканированиях и брандмауэре, которая может пригодиться при устранении неполадок. Администратор может попросить пользователя включить или настроить эти журналы, а затем экспортировать их.
Журнал пакетов	Содержит сведения о входящих и исходящих пакетах данных, переданных через порты компьютера. По умолчанию журнал пакетов выключен. На управляемом клиенте невозможно включить журнал пакетов без соответствующего разрешения администратора. На неуправляемом клиенте можно включить журнал пакетов. См. "Включение журнала пакетов" на стр. 119.
Журнал угроз	Содержит записи о вирусах и угрозах безопасности, таких как программы-шпионы и программы показа рекламы, которыми был заражен компьютер. Угрозы безопасности включают ссылку на веб-страницу Symantec Security Response, на которой имеются дополнительные сведения. См. "Управление файлами, помещенными в карантин, на компьютере" на стр. 73.

Журнал	Описание
Журнал сканирования	Содержит записи обо всех операциях сканирования, выполненных на компьютере.
Журнал безопасности	Содержит информацию о действиях, которые могут подвергнуть компьютер опасности. Например, может появиться информация о таких действиях, как атаки типа "отказ в обслуживании", сканирование портов и изменение исполняемых файлов. Кроме того, в журнале безопасности отображаются результаты проверки целостности хоста.
системный журнал	■ Защита от вирусов и программ-шпионов: содержит сведения о системных операциях на компьютере, связанных с вирусами и угрозами безопасности. Эти сведения включают информацию об изменениях конфигурации, ошибках и файле описаний. ■ Превентивная защита: содержит информацию о системных операциях на компьютере, связанных с SONAR. ■ Управление клиентами: содержит сведения обо всех произошедших на компьютере операционных изменениях. Изменения могут включать следующие действия: ■ запуск или остановка службы; ■ обнаружение компьютером сетевых приложений; ■ настройка ПО.
журнал защиты от изменений	Содержит информацию о попытках изменения приложений Symantec на компьютере. Эти записи содержат сведения о попытках, обнаруженных защитой от изменений или обнаруженных и пресеченных ею.
Журнал угроз	Содержит информацию об угрозах, обнаруженных SONAR на компьютере. SONAR обнаруживает любые файлы, которые ведут себя подозрительно. Также SONAR обнаруживает изменения системы.
Журнал трафика	Содержит события, касающиеся трафика брандмауэра и системы предотвращения вторжений. Также в этот журнал заносятся сведения о подключениях компьютера к сети. При включенном трассировщике угроз с помощью журналов предупреждения последствий использования эксплойтов сети и хоста можно трассировать трафик до его источника и блокировать возможные сетевые атаки. С помощью этих журналов можно узнать о том, когда и почему был блокирован доступ компьютера к сети. Дополнительные сведения см. в статье базы знаний Что такое трассировщик угроз?

См. "Просмотр журналов" на стр. 119.

Просмотр журналов

В журналах, которые клиент ведет на компьютере, хранятся сведения о произошедших событиях.

Как просмотреть журнал

1. На боковой панели клиента щелкните **Показать журналы**.
2. Нажмите кнопку **Показать журналы** и выберите журнал для просмотра в раскрывающемся меню.

   В зависимости от типа установки, некоторые технологии защиты могут не отображаться.

См. "Сведения о журналах" на стр. 117.

Включение журнала пакетов

По умолчанию включены все журналы предупреждения последствий использования эксплойтов сети и хоста и журналы управления клиентами, кроме журнала пакетов. На неуправляемых клиентах можно включать и выключать журнал пакетов.

На управляемых клиентах администратор может разрешить включение и выключение журнала пакетов.

См. "Сведения о журналах" на стр. 117.

Как включить журнал пакетов

1. На странице **Состояние** рядом с разделом **Предупреждение последствий использования эксплойтов сети и хоста** выберите **Параметры** и затем **Изменить параметры**.
2. Нажмите **Журналы**.
3. Выберите пункт **Включить журнал пакетов**.
4. Нажмите кнопку **ОК**.

Алфавитный указатель

З

И

К

Л

Н

О

П

Р

С

Т

У

Ф

Ц

Ч

Э