



Информационный бюллетень

Outpost Network Security 3.2

Краткое представление

При выборе корпоративных решений по обеспечению компьютерной безопасности организации отдают приоритет надежности, эффективности и экономической привлекательности продуктов. Outpost Network Security 3.2 (ONS 3.2) – разумный выбор, когда требуется обеспечить контроль над издержками и в то же время сохранить высокий уровень сетевой безопасности. Низкая стоимость защиты рабочего места, простота внедрения, обслуживания и настроек, быстрая и эффективная работа с минимальной нагрузкой на систему, гибкость и разнообразие индивидуальных возможностей настроек в сочетании с передовыми технологиями, удостоившимися многих наград, делают ONS идеальным решением для защиты электронных активов вашей фирмы.

Благодаря Outpost Network Security 3.2 ваша организация будет защищена на всех фронтах от любого возможного вида посягательств: хакеров, вирусов и прочего зловредного ПО, атак через Интернет и почтовые системы, вынужденные простои в работе, потери конфиденциальных данных и нецелевого посещения Интернет сайтов сотрудниками. Механизм центрального управления наделяет Вас легкой в использовании, нетребовательной защитой рабочих станций для организаций с ограниченными возможностями штатного обслуживания.

Вызов для небольших организаций

Бурное развитие экономики породило экспоненциальный рост атак на электронный документооборот и другие ценные корпоративные данные, заставляя организации пересмотреть действующие способы защиты критических для развития бизнеса информационных процессов. Уязвимости в установленных на корпоративные системы компьютерных программах представляют опасность распространения неизвестных вирусов и атак «нулевого дня». Для недопущения таких инцидентов требуется своевременное вмешательство администраторов и установка соответствующих патчей (исправлений) для закрытия возможностей вторжения. Эксперты отмечают значительный рост вирусов с возможностями мутации и полиморфного изменения своего содержимого, которые не могут быть выявлены традиционными методами сопоставления сигнатур. Разработанные с применением сложных технологий Трояны с элементами руткитов требуют применения новых и более продвинутых средств анализа и сдерживания. Человеческий фактор продолжает оставаться одним из главных источников угроз: сотрудники часто подвергают свои компании незримой опасности, посещая опасные веб-сайты и копируя конфиденциальную информацию на «флешку» и впоследствии теряя ее по дороге домой (не говоря уже о продаже ее содержимого конкуренту).

Набирающие обороты социальные сети не в последнюю очередь представляют большие неудобства для многих организаций, когда сотрудники часами проводят в них рабочее время, просматривая видео и переписываясь с друзьями. В то время как сотрудникам требуется обеспечить контроль и защиту рабочего места, сетевые администраторы и сотрудники IT отделов поставлены перед другой немаловажной задачей – корректной настройкой и своевременным обновлением ПО для обеспечения постоянной и надежной защиты от последних угроз. Даже небольшим компаниям с парком от двадцати машин требуется централизованный механизм установки, конфигурирования и обслуживания удаленной защиты рабочих станций, чтобы не вынуждать администраторов проводить долгое время индивидуально у каждого компьютера, имея при этом специализированное образование.

Решение Outpost Network Security 3.2

Кратко о продукте

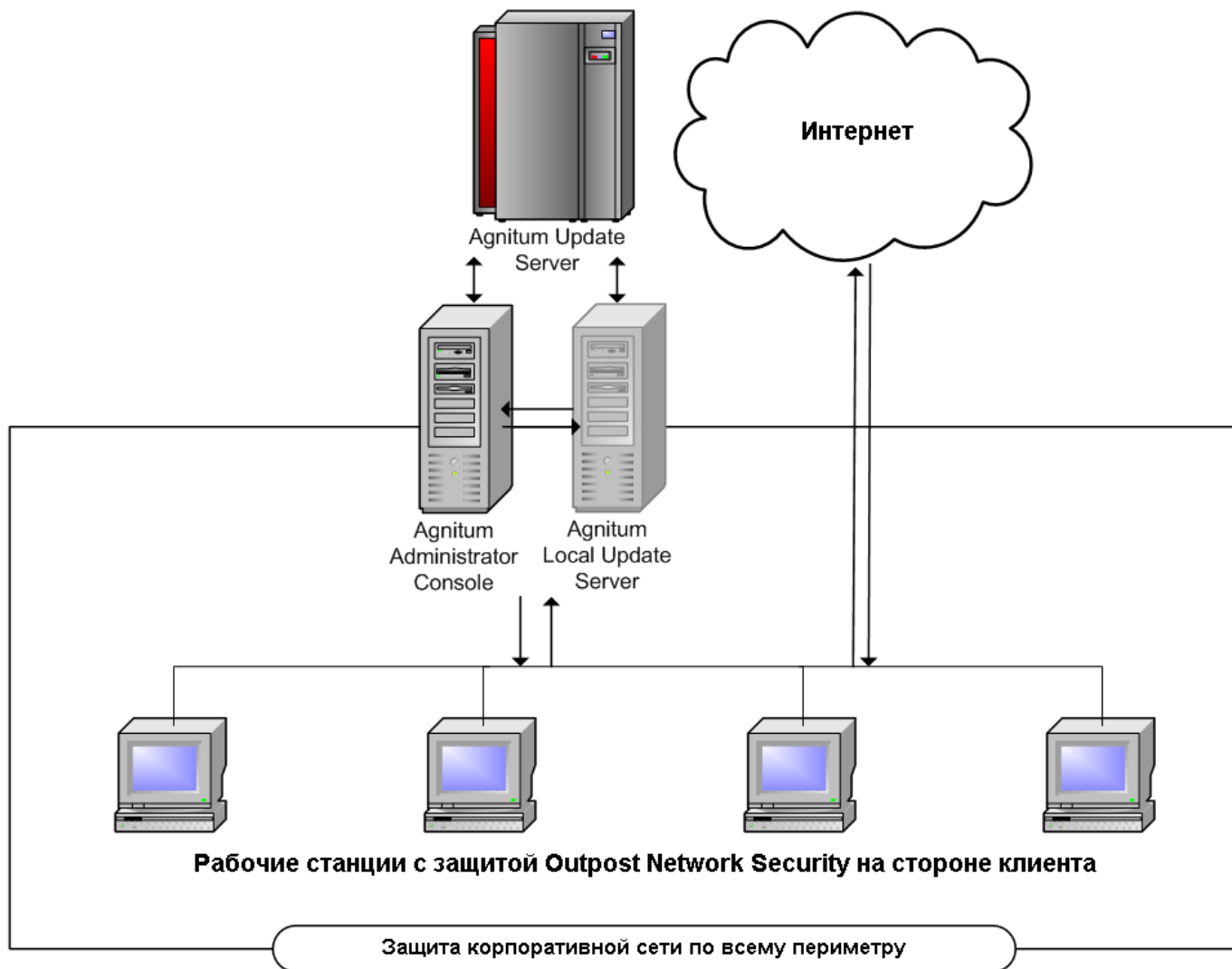
После установки Outpost Network Security, программа создает безопасную сетевую среду, защищая все элементы интрасети – от корпоративного сервера до всех подключенных рабочих станций. Защитные инструменты, установленные на клиентских машинах, работают в фоновом режиме, защищая рабочие станции от последних видов опасностей и гарантируя нераспространение вредоносного кода внутри организации. Защита рабочих станций устанавливается централизованным образом с единого контрольного пульта, доступ к которому может быть осуществлен с любого подключенного рабочего места. Это позволяет отведенному сотруднику удаленно контролировать защиту локальных пользователей, менять и назначать настройки, выполнять защитные задачи, такие как удаленные вирусные проверки по сети и изменяя политики безопасности «на лету». Outpost Network Security является идеальным выбором для организаций с:

- количеством рабочих станций от 7 до 500
- сотрудниками, часто выезжающими из офиса или не включенными в штат работниками (командировки, удаленная работа)
- несколькими удаленными друг от друга филиалами.

Ключевые моменты защиты ONS

- Автоматизированная проверка на вирусы и шпионское ПО
- Вирусная проверка по требованию позволяет просканировать удаленные рабочие станции на присутствие вредоносного кода
- Брандмауэр с фильтрацией трафика в обоих направлениях контролирует соединения и защищает от внутренних и внешних атак
- Контроль подключения USB – устройств препятствует утечке корпоративной информации
- Модуль "Защита системы" защищает системные файлы и реестр входящих в сеть ПК от вторжения и повреждения
- Контроль перемещений в Интернете гарантирует, что сотрудники не будут посещать опасные или запрещенные ресурсы
- Защита внутренних компонентов программы препятствует несанкционированному отключению
- Мониторинг процессов и сетевой активности позволяет получить информацию по удаленным событиям в режиме реального времени
- Упрощенный аудит удаленных систем благодаря удаленному доступу к журналу событий.

Outpost Network Security 3.2 защищает цифровой периметр вашей организации



Основные преимущества Outpost Network Security 3.2

Отсутствие инцидентов

Информация представляет собой самый ценный актив любой организации. Outpost сохраняет целостность и неприкосновенность ваших данных благодаря наличию таких мощных инструментов безопасности, как:

- **Антивирус для препятствия распространению вредоносного кода внутри предприятия**

Сканер безопасности, сертифицированный по VB100, содержит базы вирусных и шпионских программ для защиты от вредоносного кода внутреннего (например, поступившего по электронной почте) и внешнего происхождения (например, передающегося через зараженный flash-носитель). Администратор может начать произвольную проверку любого сетевого компьютера по своему желанию и произвести централизованное сканирование всех и каждого ПК по своей инициативе.

- **Брандмауэр с двусторонней фильтрацией для защиты сети**

Уникальные технологии передового сетевого экрана (брандмауэра), заложенные в основу ONS, гарантируют безопасность и бесперебойность работы компьютерной сети организации. Сочетая такие защитные возможности, как препятствие вторжению для охраны целостности сетевого трафика и защиты от враждебных подключений, фильтрация на основе пакетов и приложений для блокировки нежелательных или опасных соединений, защита от запуска веб-скриптов для блокировки опасных элементов во время просмотра сотрудниками Интернет-страниц, Outpost Network Security 3.2 является идеальным решением для противодействия внешним и внутренним врагам в современной бизнес-среде.

- **Модуль "Защита системы"**

"Защита системы" предоставляет администратору сети возможность настроить список защищаемых системных приложений и другие важные опции для конфигурирования защиты, включая настройки реестра, свойства сети, доступ к хосту, взаимодействие плагинов Adobe Flash и Reader и других уязвимых приложений. Любая специальная программа может стать объектом "Защиты системы", тем самым администратор может обезопасить тот или иной системный объект от сетевых угроз.

- **Веб-контроль**

Администратор имеет возможность превентивно блокировать доступ к нежелательным или потенциально опасным веб-страницам по ключевым словам в URL и в теле страниц.

- **Блокиратор доступа к USB-устройствам**

Outpost Network Security снижает риск утечки корпоративной информации благодаря новому инструменту, позволяющему блокировать использование внешних устройств хранения данных.

Простое развертывание и удобное обновление

- **Централизованная установка для снижения нагрузки на IT-отдел**

Благодаря простым и интуитивным средствам удаленного развертывания, массовая установка клиентской защиты осуществляется в считанные минуты. Для этого администраторам лишь потребуется в окне, отображающем сетевую структуру компании, выбрать конкретные ПК для установки клиентского агента.

- **Централизованное и автономное обновления баз**

Ежедневное обновление антивирусных баз для поддержания актуальности защиты осуществляется по сети из единого источника – будь то сервер Agnitum, локальный сервер обновлений или локальная папка с обновленными базами.

Централизованное управление

- **Разделение по группам для более точной настройки прав**

Все подконтрольные машины можно объединить в несколько групп, имеющих собственные настройки безопасности. Такая возможность позволяет администраторам более точно управлять и назначать различные правила безопасности в зависимости от подверженности риску, прав доступа к определенным сайтам, запускаемых приложений и т.д. для разных групп пользователей. Так, например, можно указать более жесткие ограничения для мобильных сотрудников, которые подвержены риску заражения извне.

- **Удаленное управление максимально облегчает задачи администратора**

В новой версии Outpost Network Security управление клиентскими машинами может быть осуществлено из любой точки в пределах организации, включая одну из клиентских машин – при условии, что на ней установлена административная консоль. Удаленная консоль позволяет настраивать такие функции клиентской защиты, как назначение прав доступа для приложений, управление работой различных модулей продукта, а также указывать черные списки блокируемых Интернет-адресов или запускать антивирусное сканирование по требованию.

Прозрачность и информативность удаленных событий

- **Удобный контроль за действиями удаленных машин**

После того как корпоративная сеть налажена и программы установлены, администраторам системы бывает очень тяжело контролировать работу клиентских ПК. Outpost постарался обойти это ограничение, предложив администратору удобное средство просмотра текущих сетевых и системных событий на любом компьютере сети. Это средство также предоставляет возможность быстрого изменения текущих правил для приложений и позволяет в экстренных случаях аварийно завершать работу активных программ на клиентских ПК.

- **Ведение удаленного протоколирования для лучшего понимания прошлых событий**

Благодаря подробным сведениям, предоставляемым журналом ведения прошлых событий системы ONS, администратор всегда будет в курсе того, что делал ранее тот или иной компьютер в сети. Это средство позволяет администратору моментально выявить проблему или сбой в работе парка обслуживаемых машин и быстро скорректировать ситуацию, не покидая своего рабочего места.

Непрерывная защита – быстрая и нетребовательная к ресурсам

- **Более быстрая защита с технологией SmartScan**

В результате введения множественных оптимизаций и использования уникальных технологий, способствующих росту производительности, клиентские модули Outpost работают в теновом режиме и не отнимают существенных ресурсов системы. Программа работает быстро и незаметно для сотрудника, а проверка на вирусы занимает до 10 раз меньше времени относительно некоторых конкурентных решений.

- **Защита, которую невозможно деактивировать**

Работа системы на стороне клиента не может быть остановлена в результате враждебных целевых атак, что гарантирует бесперебойную и постоянную защиту ПК в сети организации от всех видов новейших угроз.

Универсальная совместимость

- **Поддержка современных программ и оборудования для повсеместного использования**

Outpost Network Security 3.2 поддерживает все современные 32- и 64-битные операционные системы, включая Windows 7, Windows Vista SP2, Windows Server 2008 и Windows Server 2008 R2.

Основные возможности Outpost Network Security 3.2

Сохранность и конфиденциальность корпоративной информации

- **Надежная защита от вредоносных программ**

Outpost Network Security позволяет защитить вашу организацию от всех видов вредоносных программ, включая вирусы, шпионское ПО, Трояны, черви и прочие виды угроз, оставаясь на страже рабочих станций вашей организации 24 часа в сутки 7 дней в неделю. Защита осуществляется автоматически, под управлением сетевого администратора организации, и не зависит от уровня компьютерной грамотности сотрудников. Проверка удаленных машин «на лету» осуществляется автоматически в фоновом режиме, в то время как файловый сканер, оснащенный передовой технологией упреждающей проверки SmartScan, позволяет быстро и эффективно проверить такие подверженные заражению области, как системные папки Windows, локальные и общие диски, съемные носители.

- **Бесперебойная работа сети**

Встроенный в ONS брандмауэр, работающий на стороне клиента, защищает входящие и исходящие соединения. Он фильтрует сетевой трафик согласно правилам, назначенным администратором, и блокирует ненужные или вызванные исполнением враждебного кода сетевые соединения. Уникальный модуль отражения внутрисетевых атак позволяет защититься от вторжений типа «внедренный агент», которые нацелены на захват чужого трафика. Благодаря этому инструменту, вся информация достигает своего непосредственного получателя, и не может быть перехвачена и использована хакерами.

- **Модуль "Защита системы"**

Модуль "Защита системы", наследник более раннего компонента "Контроль объектов", защищает критически важные ветки реестра и системные файлы, предотвращая эти ключевые объекты от несанкционированной модификации и повреждения. Любая специальная программа может стать объектом "Защиты системы", тем самым администратор может обезопасить тот или иной системный объект от сетевых угроз.

- **Запрет использования USB-устройств хранения данных**

С целью препятствия распространению вирусов и других вредоносных программ из внешней среды, а также недопущения копирования и выноса внутренней информации компании, IT отделы могут запретить использование устройств USB некоторым сотрудникам организации.

- **Защита перемещений по небезопасным веб-сайтам**

С помощью ONS производительность ваших сотрудников всегда будет оставаться на высшем уровне, а риски заражения или потери информации стремиться к нулю. Программа позаботится, чтобы ваши сотрудники были ограждены от небезопасных или мошеннических Интернет сайтов, стремящихся заразить посетителей автоматически запускаемыми сценариями. Механизм также вырежет из страниц назойливую рекламу, графические баннеры, анимацию и прочее отвлекающее наполнение рекламного характера. В дополнение к этому, администратор может заблокировать для сотрудников посещение определенных веб-сайтов, которые не относятся к выполнению служебных задач.

- **Самозащита на страже офисных ПК**

ONS обладает уникальной технологией, которая гарантирует, что работа программы не может быть нарушена в результате вирусных атак, нацеленных на подрыв защитных функций системы безопасности. Никто, кроме администратора сети, не может остановить защиту ONS, что позволяет организации максимально защитить компьютеры своих работников.

Контроль и управление

- **Централизованное развертывание и администрирование**

Клиентские модули устанавливаются из центральной консоли управления путем простого выбора целевых рабочих станций. Спустя пару минут все выбранные клиенты уже работают под защитой ONS. Все последующие задачи, связанные с администрированием удаленных машин, доступны администратору с любого компьютера, подключенного в офисную сеть.

- **Разделение на группы пользователей**

Поддержка нескольких групп пользователей позволяет администраторам применять различные настройки безопасности в зависимости от отдела, где работает тот или иной сотрудник.

- **Подробные сведения об удаленных событиях**

Уникальные возможности сетевого администрирования ONS включают способность администратора просматривать отчеты по событиям на клиентских машинах в режиме реального времени. Отчеты содержат такую разноплановую информацию, как запущенные на стороне клиента программы и процессы, Интернет-адреса, к которым обращается компьютер сотрудника, и другие текущие сведения. Незавершенные соединения могут быть моментально разорваны, а новые политики безопасности созданы «на лету» для быстрого реагирования на последние виды угроз.

- **Исчерпывающий журнал прошлых событий**

Благодаря мощным инструментам протоколирования событий на стороне клиента, администраторы могут быстро понять и разрешить проблемы с соединениями, просматривать результаты вирусных проверок и получать доступ к прочей служебной информации.

Системные требования Outpost Network Security 3.2

Поддерживаемые платформы:

Outpost Network Security 3.2 поддерживает все современные 32- и 64-битные операционные системы, включая Windows 7, Windows Vista SP2, Windows Server 2008 и Windows Server 2008 R2.

Оборудование:

процессор 500 МГц или выше(x86/x64), 256 Мб ОЗУ, 100Мб свободного дискового пространства.

Изменение функциональных возможностей в зависимости от версии программы Outpost Network Security

Версия продукта	Outpost Office Firewall	Outpost Network Security 2.0	Outpost Network Security 3.0	Outpost Network Security 3.2
Брандмауэр для защиты сетевых подключений	да	да	да	да
Модуль «Антишпион» для базовой защиты	да	да	да	да
Антивирус для полной защиты от вредоносного ПО	нет	нет	да	да
Модуль «Защита системы» для защиты системных файлов и реестра	нет	нет	нет	да
Упрощенное развертывание через меню программы	нет	нет	да	да
Удаленное сканирование на вирусы по требованию	нет	нет	да	да
Защита на подключение USB-устройств	нет	нет	да	да
Веб-контроль для соблюдения корпоративной политики	нет	нет	нет	да
Обновляемый список опасных Интернет адресов	нет	нет	да	да
Разделение защищаемых узлов по типам пользователей для целенаправленной защиты	нет	да	да	да
Возможность просмотра удаленных событий в реальном времени	нет	нет	да	да
Встроенная поддержка 64-битных версий Windows	нет	нет	да	да
Поддержка всех новейших платформ, включая Windows 7 и Server 2008 R2	нет	нет	нет	да

Ваш следующий шаг

Загрузите полнофункциональную 30-дневную пробную версию Outpost Network Security 3.2 на www.network-security.ru и защитите сеть вашей организации!