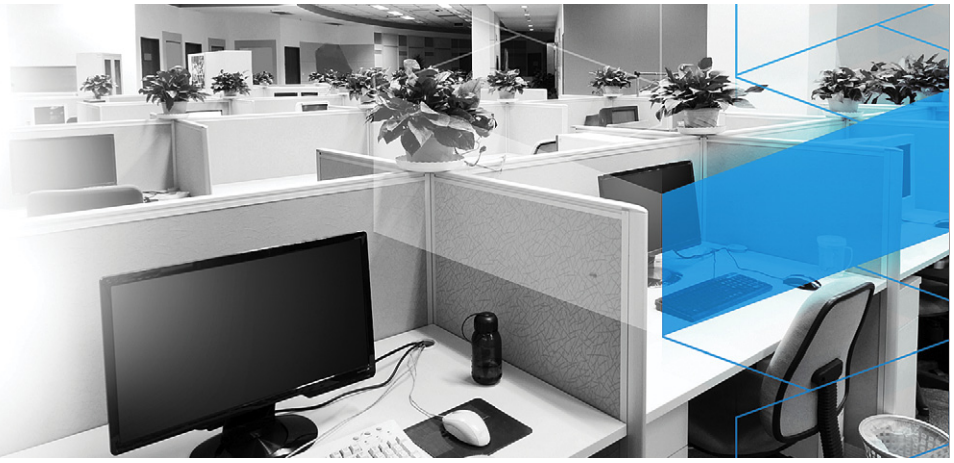
BITDEFENDER
CLIENT SECURITY



ОСНОВЫ КОММЕРЧЕСКОЙ БЕЗОПАСНОСТИ

Ко всем новым и существующим компаниям должны предъявляться одинаковые требования безопасности, независимо от масштаба предприятия. Защита интеллектуальной собственности предприятия и обеспечение сохранности данных клиентов, безусловно, важны и необходимы, однако неготовность к появлению вирусов может значительно снизить эффективность работы персонала и организации в целом. Потеря работоспособности способна парализовать небольшое предприятие или, по крайней мере, существенно замедлить его развитие.

ПРОСТОЙ УСТАНОВКИ АНТИВИРУСА НЕДОСТАТОЧНО

Вирусы постоянно развиваются и совершенствуются, чтобы обходить существующие инструменты управления безопасностью, внедренные в корпоративных сетях. Хотя установка антивирусного программного обеспечения, безусловно, является основой грамотной политики безопасности, только этого уже недостаточно для защиты сотрудников от существующих угроз. К вирусам, которые способны причинить серьезный ущерб деятельности предприятия, можно отнести следующие:

Вирусы: распространяются посредством заражения исполняемых файлов, скрытых внутри сжатых архивов, или в виде микрокоманд в легитимных документах. Полезная нагрузка вируса включает удаление файлов, шифрование данных, очистку жесткого диска и т.д.

Рекламные и шпионские программы: шпионское ПО, практически столь же опасное и разрушительное, как и вирусы, может оказаться сложно распознать и удалить. Помимо нарушения работоспособности компьютера, установки дополнительного программного обеспечения и перенаправления браузера, наиболее серьезную опасность представляет собой утечка личной и корпоративной информации. В случаях серьезного поражения вирусом может потребоваться полная переустановка системы, которая не только отнимает несколько часов, но и требует существенного объема ресурсов ИТ-инфраструктуры.

Вирусы-"черви": самореплицирующиеся программы, использующие для распространения сеть; замедляют работу сети и инфицируют систему, максимально используя уязвимости систем и приложений. Полезная нагрузка вируса может включать удаление или шифрование файлов, отправку документов по электронной почте, установку бэкдоров, "зомби" и "троянских коней".

"Троянские кони" и руткиты: "троянские кони" и руткиты маскируются под легитимные программы, но их истинная цель — обеспечить удаленный доступ к системе компьютера. После установки "троянского коня" или руткита злоумышленники получают удаленный доступ к системе, что зачастую приводит к хищению данных. Обнаружение и нейтрализация угроз такого типа вручную может занять достаточно продолжительное время и при неправильном удалении вируса может повлечь полную переустановку системы.

Почтовый спам и фишинг: незапрашиваемые рекламные материалы коммерческого характера, распространяемые по электронной почты, не только раздражают, но и представляют определенную угрозу. В отсутствие грамотно организованного управления обработка спама отнимает у пользователей слишком много времени. При некоторых фишинговых или спам-атаках во вложениях могут содержаться вредоносные программы (что может скомпрометировать внутренние данные) или ссылки на веб-сайты, запрашивающие личную информацию. Фишинг использует сходные приемы, но в этом случае пользователь перенаправляется на кажущийся легитимным веб-сайт, истинная цель которого — собрать личные сведения (данные кредитной карты или банковского счета) или поместить в систему клавиатурного шпиона для сбора критически важной информации о предприятии.

Проникновение в систему вредоносного программного обеспечения может нанести серьезный вред всем сотрудникам организации, однако, как правило, именно ИТ-департамент в наибольшей степени страдает от последствий такого проникновения. ИТ-администраторы, уже имеющие опыт удаления быстро распространяющегося вируса-"червя" или вируса, поражающего большое число систем, знают какой это длительный и трудоемкий процесс. К сожалению, именно эта задача является приоритетной в сравнении с остальными ИТ-проектами, поскольку только при условии ее выполнения возможно ограничить потерю данных и обеспечить восстановление работоспособности сотрудников в кратчайшие сроки.

ЗАЩИТА КОНЕЧНЫХ ТОЧЕК С ПОМОЩЬЮ РЕШЕНИЙ BITDEFENDER

Профилактическая защита позволяет предотвратить потерю данных и утрату работоспособности в результате воздействия вредоносного ПО. Предприятия могут надежно защитить конечные точки от вирусных атак с помощью функциональных возможностей BitDefender, позволяющих обнаруживать и предотвращать проникновение известных и новых вирусов, обеспечивающих соблюдение политик безопасности предприятия и эффективное управление ими при минимальном задействовании ресурсов ИТ-инфраструктуры.

ОСНОВНЫЕ ХАРАКТЕРИСТИКИ И ПРЕИМУЩЕСТВА

- ***Знаменитая система обнаружения, удаления и нейтрализации вирусов, шпионского и рекламного ПО, "троянских коней" и руткитов***
- ***Дает широкие возможности планирования проверок по запросу и автоматических проверок с целью обнаружения новых проникновений вирусов***
- ***Оптимизированное сканирование с использованием идентификации файлов по каждому пользовательскому сеансу и их повторное сканирование при открытии нового сеанса или в случае заражения системы***
- ***Помещение инфицированных и подозрительных файлов в карантин в целях минимизации вероятности заражения и последующего безопасного анализа***
- ***Настройка и управление на основе политики***
- ***Персональный брандмауэр для защиты удаленных и перемещаемых пользователей***
- ***Защита от спама на уровне системы с использованием постоянно обновляемых "черных" и "белых" списков и байесовской самообучающейся системы для распознавания нового спама, который не блокируется стандартными фильтрами***
- ***Настраиваемая фильтрация содержимого позволяет распознавать критически важную информацию в целях минимизации утечки данных***
- ***Снижение стоимости ресурсов и сокращение накладных расходов при управлении несколькими клиентами посредством консоли централизованного управления.***
- ***Обеспечивает возможность удаленной настройки, аудита, установки и удаления приложений из любой клиентской или серверной системы в рамках сети***

Bitdefender

ТЕХНОЛОГИИ BITDEFENDER

Все решения BitDefender используют патентованную технологию B-HAVE, с помощью которой выполняется анализ поведения возможного вредоносного кода в пределах виртуального компьютера, благодаря чему исключаются ложные обнаружения и значительно повышается уровень распознавания новых и неизвестных вредоносных программ.

В целях более качественного реагирования на появление новых методик рассылки спама лаборатория BitDefener разработала технологию NeuNet — мощный инструмент для фильтрации спама. В ходе апробации технологии NeuNet в лабораторных условиях была использована серия спам-сообщений, поэтому система способна обучаться распознаванию новых видов спама, анализируя сходство с обработанными ранее спам-сообщениями.

СИСТЕМНЫЕ ТРЕБОВАНИЯ

Решение BitDefender Client Security включает два основных компонента: Business Client для Windows-систем и агент управления Management Agent.

BitDefender Business Client для Windows

Минимальные требования к процессору:
Совместимый с Intel Pentium процессор 800 МГц

Минимальные требования к ОЗУ:
- 256 МБ ОЗУ для Windows 2000 и Windows XP
- 512 МБ ОЗУ для Windows Vista и Windows 7

Минимальные требования к дисковому пространству: 200 МБ (400 МБ для установки)

Операционная система:
- Windows 2000 Professional с SP 4 и накопительным пакетом обновлений 1 версии 2
- Windows XP SP2
- Windows Vista
- Windows 7

Bit Defender Management Agent

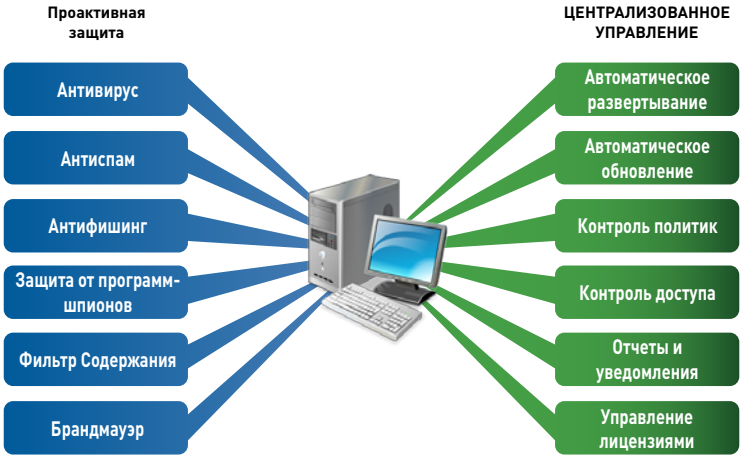
Минимальные требования к процессору:
- Процессор, совместимый с Intel Pentium

Минимальные требования к ОЗУ:
- ОЗУ 256 МБ для Windows 2000, Windows XP, Windows 2003
- ОЗУ 512 МБ для Windows Vista, Windows 2008, Windows 7

Минимальные требования к дисковому пространству: 100 МБ

Операционная система:
- Windows 2000 Professional с SP 4 и накопительным пакетом обновлений 1 версии 2
- Windows 2000 Server SP4
- Windows XP SP2
- Windows Server 2003 SP2
- Windows Vista
- Windows 2008 Server
- Windows 7
- Linux 2.4.x или 2.6.x с библиотеками glibc 2.3.1 (или более поздней версии) и libstdc++5 из gcc 3.2.2 (или более поздней версии)

Bitdefender



BitDefender Client Security обеспечивает функции безопасности и управления клиентами на нескольких уровнях

УЛУЧШЕННОЕ ПРОФИЛАКТИЧЕСКОЕ РАСПОЗНАВАНИЕ

Системы сканирования BitDefender признаны ведущими органами сертификации, включая ICSA Labs, Virus Bulletin и West Coast Labs, благодаря не имеющей аналогов профилактической защите от вредоносного ПО. BitDefender Client Security обеспечивает расширенную защиту на нескольких уровнях: антивирусная защита, фильтрация спама, фишинга и содержимого, защита от шпионских программ, функции распознавания "троянских коней" и руткитов, а также полнофункциональный персональный брандмауэр.

НАСТРОЙКА И УПРАВЛЕНИЕ ДЕТАЛЬНЫМ СКАНИРОВАНИЕМ

BitDefender Client Security предоставляет несколько технологий сканирования, позволяющих распознавать вредоносный код в целях защиты целостности компьютеров и рабочих станций, подключенных к корпоративной сети. Различные функции сканирования позволяют поддерживать целостность системы и минимизировать негативные последствия для работы пользователей.

Автоматически при включении предоставляет функции распознавания вирусов в режиме реального времени при добавлении или извлечении пользователем документов из списка или библиотеки документов.

по запросу позволяет выполнять сканирование системы по графику, запланированное на рабочие часы с небольшой нагрузкой во избежание нарушения работы или доступа к системе.

Настройка сканирования по графику обеспечивает возможность планирования настраиваемых событий для сканирования по запросу и задач обновления, что позволяет свести к минимуму потенциальные перебои в работе сервера или системы в пиковые рабочие часы.

Помещение инфицированных и подозрительных файлов в карантин — подозрительные файлы изолируются в зоне карантина, после чего может быть выполнена очистка этих файлов, либо они сохраняются в карантине для дальнейшего анализа, восстанавливаются в исходное расположение по завершении проверки или направляются непосредственно в антивирусную лабораторию BitDefender для изучения.

АВТОМАТИЧЕСКИЕ ОБНОВЛЕНИЯ

Вирусные сигнатуры обновляются каждый час, а развертывание обновлений продуктов могут выполняться без нарушения стандартной работы сети во время планового технического обслуживания, благодаря чему обеспечивается соответствие развертываемых решений Client Security новейшим разработкам в сфере антивирусной безопасности.

ИНТЕГРАЦИЯ С ПЛАТФОРМОЙ ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ BITDEFENDER

Управление большим числом рабочих станций легко осуществляется посредством платформы централизованного управления BitDefender. Таким образом ИТ-администраторам предоставляется обзор угроз проникновения вредоносного ПО в масштабах организации и инструменты профилактической защиты сетевых ресурсов. Сервер управления BitDefender Management Server представляет собой центр управления удаленной установкой, настройкой и генерацией отчетности по всем продуктам BitDefender из линеек Clients, Server и Gateway, развернутых в рамках предприятия. Он также оповещает администраторов о выполнении сканирования, обнаружении вирусов и задачах обновления посредством многоцелевого модуля оповещения.

ВСЕСТОРОННЯЯ ЗАЩИТА

BitDefender Client Security представляет собой лишь один из компонентов комплексной системы решений, обеспечивающих полную защиту сети от шлюза до рабочей станции. Проактивные многоплатформенные решения BitDefender выполняют обнаружение и предотвращают проникновение вирусов, шпионских и рекламных программ, а также "троянских коней", способных скомпрометировать целостность сети.