BITDEFENDER
ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ ДЛЯ РЕШЕНИЙ КОРПОРАТИВНОЙ БЕЗОПАСНОСТИ

Одной из наиболее сложных задач для любого ИТ-департамента является осуществление контроля и обзора состояния безопасности предприятия. К сожалению, многие организации не располагают специализированными ресурсами, с помощью которых осуществляется разработка и управление стратегиями сетевой безопасности, что обусловлено высокой стоимостью таких ресурсов. Предприятия среднего и малого бизнеса в еще большей степени ограничены условиями бюджета, и задачи в сфере ИТ зачастую выполняются специалистами, занимающимися, кроме этого, решением и других задач. При отсутствии четких приоритетов реализация эффективной программы безопасности в рамках предприятий малого и среднего бизнеса становится довольно сложной задачей.

По мере роста организации появление новых сотрудников или внедрение новых систем с целью расширения деятельности может вызвать увеличение числа векторов атаки, используемых вредоносными программами для проникновения в корпоративную сеть. В целях профилактической защиты ИТ-отделы должны обеспечить надлежащий контроль, чтобы ограничить последствия несанкционированного использования мошеннических приложений, вредоносного кода и интернет-ресурсов (например, приложений Web 2.0), которые способны поставить предприятие под удар.

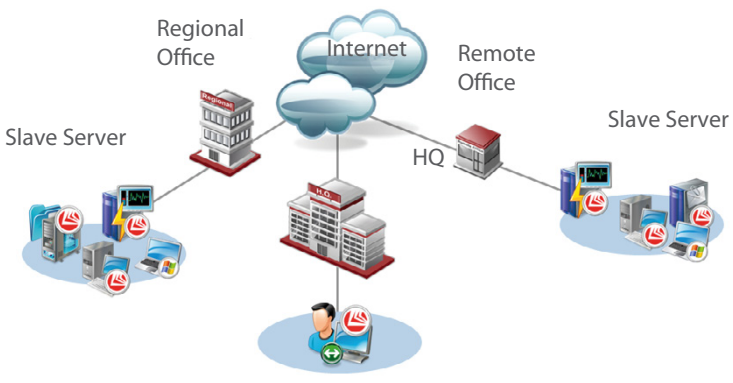
ИСПОЛЬЗОВАНИЯ РЕШЕНИЙ БЕЗОПАСНОСТИ ДЛЯ КОНЕЧНЫХ ТОЧЕК НЕДОСТАТОЧНО

Антивирусная среда, развертываемая на компьютерах и рабочих станциях предприятия, является основой для эффективной политики безопасности. Однако сегодня этого уже недостаточно для защиты персонала от угроз проникновения вирусов. Вирусы постоянно развиваются и совершенствуются, чтобы обходить существующие решения безопасности и быстро распространяться в отсутствие проверки с помощью средств контроля. Решения антивирусной безопасности BitDefender представляют собой комплексные инструменты обнаружения и распознавания вирусов, которые можно использовать для защиты неуправляемых рабочих станций и серверов, удаленного обнаружения и удаления несанкционированных приложений, а также для настройки системных параметров, что позволяет в итоге свести к минимуму последствия распространения вредоносных программ по сети.

ЗАЩИТА СИСТЕМ ПРЕДПРИЯТИЯ С ПОМОЩЬЮ РЕШЕНИЙ BITDEFENDER

С помощью консоли централизованного управления BitDefener предприятия могут внедрить объединенную платформу управления удаленной установкой, настройкой и отчетностью для всех продуктов BitDefender из линеек Clients, Server и Gateway, развертываемых в сети. Решение для централизованного управления BitDefender включает:

- Обзор событий, связанных с вредоносным ПО в масштабах сети для ИТ-администраторов
- Профилактический аудит оборудования и программного обеспечения, задействованного в сети
- Удаленная настройка и управление системными параметрами клиента и сервера
- Отчет о событиях, связанных с вредоносным ПО, в целях выявления масштаба и тенденций распространения вируса
- Инструменты измерения эффективности программы антивирусной безопасности предприятия



ОСНОВНЫЕ ХАРАКТЕРИСТИКИ И ПРЕИМУЩЕСТВА

- ***Снижение стоимости ресурсов и накладных расходов, связанных с управлением несколькими конечными точками и серверами***
- ***Объединение нескольких проблем по запросу с возможностью их решения "одним нажатием"***
- ***Обеспечивает возможность удаленной настройки, аудита, установки и удаления приложений с любой конечной точки или сервера в рамках сети***
- ***Сетевое обнаружение конечных точек, на которых не установлены антивирусные решения, обеспечение удаленного развертывания решения Client Security***
- ***Настраиваемые политики безопасности с предварительно определенными шаблонами, упрощающими реализацию политики***
- ***Интегрируется с Active Directory в целях максимально эффективного использования существующих групповых политик организации и структуры домена Windows.***
- ***Обеспечивает возможность удаленной настройки с любого компьютера в сети предприятия посредством консоли управления***
- ***Масштабируемая архитектура "главный-подчиненный" обеспечивает управление шлюзами, серверами и конечными точками, находящимися в разных физических расположениях***

Bitdefender

ПРОВЕРКА КОНЕЧНЫХ ТОЧЕК И СЦЕНАРИИ УПРАВЛЕНИЯ

Сервер управления BitDefender Management Server использует язык сценариев инструментария управления Windows (WMI) для аудита и управления конечными точками и серверами. В целях автоматизации удаленного управления в систему включено свыше 30 шаблонов сценариев WMI. Кроме того, предусмотрены сотни общедоступных сценариев массовой обработки: завершение приложений и процессов, установка и удаление программ, перезагрузка и выключение рабочих станций, включение и выключение автозапуска, а также доступ к съемным USB-носителям.

ВСЕСТОРОННЯЯ ЗАЩИТА

Решение для централизованного управления BitDefender является основным компонентом 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

СИСТЕМНЫЕ ТРЕБОВАНИЯ

Решение для централизованного управления BitDefender включает три основных компонента: сервер управления Management Server, поддерживающий инфраструктуру централизованного управления для всех решений BitDefender; консоль управления, служащую пользовательским интерфейсом и сервер обновлений для загрузки и распределения обновлений продукта и вирусных сигнатур.

Минимальные требования к процессору: Intel Pentium 1 ГГц (рекомендуется процессор 2 ГГц)
Минимальные требования к ОЗУ: 512 МБ (рекомендуется 2 ГБ)
Минимальные требования к дисковому пространству: 1,5 ГБ (рекомендуется 2,5 ГБ), 3 ГБ для обновлений

Операционная система

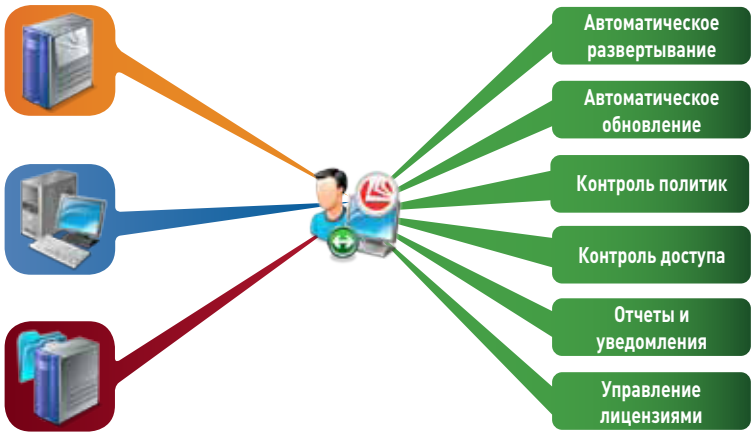
- Windows 2000 Professional SP4
- Windows 2000 Server SP4
- Windows XP SP2
- Windows Server 2003 SP2
- Windows Vista
- Windows 2008 Server
- Windows 7

База данных

- Microsoft SQL Server 2005 или Microsoft SQL Express Edition (бесплатная версия)

Все товарные знаки, торговые наименования и продукты, упоминаемые в настоящем документе, являются собственностью их соответствующих владельцев. Все права защищены. © BitDefender, 2010 г.

Bitdefender



Консоль BitDefender обеспечивает возможность централизованного управления шлюзами, конечными точками и критическими серверами

ВОЗМОЖНОСТИ ВИЗУАЛЬНОГО ДОСТУПА И УДАЛЕННОГО УПРАВЛЕНИЯ

Консоль управления BitDefender отличается простотой развертывания и удобством управления. Централизованный интерфейс предоставляет обзор состояния безопасности предприятия, возможность конфигурации удаленных конечных точек и реализацию политик безопасности. В консоли управления объединены данные об угрозах и состоянии системы, получаемые со всех управляемых рабочих станций на основе Unix и Windows, а также с серверов в сети предприятия. Возможно быстрое выявление событий и критических проблем в конечных точках и их разрешение "одним нажатием", что позволяет свести к минимуму время администрирования и отклика на критически важные события.

Решения BitDefender на основе UNIX-систем используют отдельный интерфейс удаленного веб-администрирования в работе BitDefender Security for Mail Servers или BitDefender Security for Samba File Servers. Помимо этого интерфейса для опытных пользователей, предпочитающих стандартный интерфейс администрирования инфраструктуры сети, предусмотрено использование командной строки.

АРХИТЕКТУРА "ГЛАВНЫЙ-ПОДЧИНЕННЫЙ" СЕРВЕРА УПРАВЛЕНИЯ

Управление централизованной системой синхронизации политик, продуктов и обновлений в масштабах предприятия осуществляется посредством главного сервера управления. Главный сервер обеспечивает централизованное интеллектуальное распределение обновлений в локальной или удаленно управляемой сети, к которой подключен локальный подчиненный сервер управления. Такая архитектура обеспечивает доступность обновлений для локальных ресурсов в целях оптимизации использования сети.

АВТОМАТИЧЕСКОЕ ИЛИ ЗАПЛАНИРОВАННОЕ РАСПРОСТРАНЕНИЕ ОБНОВЛЕНИЙ

Сервер управления BitDefender обеспечивает интеллектуальное централизованное распределение новых вирусных сигнатур и обновлений для продуктов. Установка обновлений может выполняться автоматически каждый час по мере их поступления, либо планироваться на непиковый период во избежание снижения производительности и излишней нагрузки на сеть.

УПРАВЛЯЕМЫЕ ПОЛИТИКИ БЕЗОПАСНОСТИ НА ОСНОВЕ СТРУКТУРЫ ДОМЕНА WINDOWS

В процессе интеграции в Active Directory существующая структура домена Windows и групповые политики предприятия используются максимально эффективно. Как альтернатива управлению группами рабочих станций в рамках сервера управления могут применяться политики безопасности — путем непосредственного выбора пользователей или групп пользователей из Active Directory. Сервер управления BitDefender выполняет обнаружение неуправляемых рабочих станций в целях их идентификации и последующей передачи их под управление автоматизированной удаленной среды, либо исключения отдельных рабочих станций из общих политик безопасности.