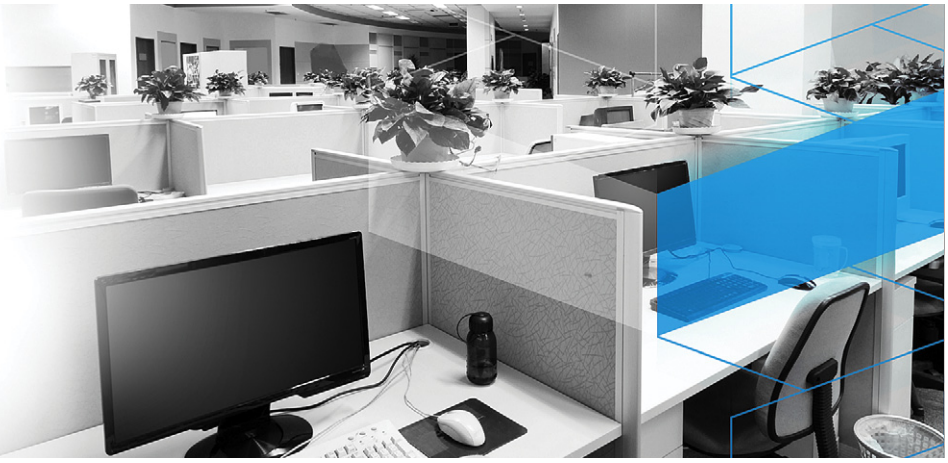
BITDEFENDER
АНТИВИРУС SCANNER ДЛЯ UNIX-СИСТЕМ



БЕЗОПАСНОСТЬ LINUX ТЕПЕРЬ НАХОДИТСЯ ПОД УГРОЗОЙ

Операционные системы Linux на протяжении многих лет считались менее уязвимыми по сравнению с системами Windows, но в итоге миф об их "иммунитете" против вирусных атак полностью развеян. Устойчивость платформ Linux на ранних стадиях развития системы была обусловлена недостаточностью доступа к корневым каталогам, при наличии которого вредоносное ПО может проникать в систему, способностью сообщества разработчиков Linux быстро исправлять уязвимости и сравнительно редким использованием Linux в корпоративных сетях. В свете вышеперечисленного системы Linux не являлись приоритетной мишенью для создателей вредоносных программ. Однако на данный момент приоритеты активно изменяются ввиду быстро растущей популярности платформ Linux среди предприятий.

Многие организации все чаще предпочитают использовать компьютеры на основе Unix-систем в качестве более экономичной альтернативы. Такие стандартные службы, как электронная почта и веб-службы, также доступны для пользователей компьютеров на основе Unix-систем, как и их аналоги на основе Windows. Использование конечных точек на основе Unix-систем рядовыми сотрудниками становится все более простым и удобным (особенно после появления графических интерфейсов пользователя и приложений, совместимых с Windows-системами), и это сделало возможным их использование в локальных сетях малых и средних предприятий. При отсутствии надлежащей защиты эти системы в той же мере, что и Windows-системы, подвержены проникновению вредоносного ПО в локальную сеть организации посредством совместно используемых файлов, кросс-платформенных вирусов, вирусов-"червей" или вложений электронной почты.

ЗАЩИТА КОНЕЧНЫХ ТОЧЕК НА БАЗЕ UNIX-СИСТЕМ С ПОМОЩЬЮ РЕШЕНИЙ BITDEFENDER

Профилактическая защита позволяет предотвратить потерю данных и утрату работоспособности в результате действия вредоносного ПО. Предприятия могут надежно защитить конечные точки на основе Unix-систем 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.

АНТИВИРУСНЫЙ СКАНЕР BITDEFENDER ДЛЯ UNIX-СИСТЕМ

BitDefender Антивирус Scanner для Unix-систем представляет собой многофункциональный сканер по запросу для систем Linux и FreeBSD. Автономный сканер обеспечивает защиту дисковых разделов Unix- и Windows-систем путем сканирования на наличие вирусов и шпионских программ. Удобный графический интерфейс пользователя дополнен многофункциональным интерфейсом командной строки, полностью поддерживающим инструментарий сценариев операционной системы. Сканер работает автономно, локальный сервер централизованного управления или обновления для его работы не требуется.

ИНТЕГРАЦИЯ РАБОЧЕЙ СТАНЦИИ

BitDefender Антивирус Scanner для Unix-систем оснащен графическим интерфейсом пользователя, обеспечивающим доступ к функциям сканирования прямо из меню приложений или посредством командной строки (для более опытных пользователей). Сценарий и расширения приложений обеспечивают бесшовную интеграцию выбранного пользователем диспетчера файлов, почтового или новостного клиента с системой сканирования BitDefender. В большинстве случаев для этого достаточно щелкнуть мышью, нажать на комбинацию клавиш

ОСНОВНЫЕ ХАРАКТЕРИСТИКИ И ПРЕИМУЩЕСТВА

- ***Знаменитая система обнаружения, удаления и нейтрализации вирусов, шпионского и рекламного ПО, "троянских коней" и руткитов***
- ***Удобный графический интерфейс пользователя дополнен функциональным интерфейсом командной строки***
- ***Интеграция рабочего стола с меню выбранных диспетчеров файлов***
- ***Интеграция на основе сценариев или расширений с различными приложениями и службами***
- ***При сканировании почтового ящика выполняется сканирование вложений электронной почты. Функции сканирования поддерживают выбранные расширения почтового клиента***
- ***Сканер поддерживает свыше 80 форматов файлов упакованных архивов***
- ***Помещение инфицированных и подозрительных файлов в карантин в целях минимизации вероятности заражения и последующего безопасного анализа***
- ***Совместимость со всеми основными платформами на основе Unix-систем с поддержкой пакетов rpm, deb и универсальных пакетов .tar.run.***

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.

ВСЕСТОРОННЯЯ ЗАЩИТА

BitDefender Антивирус Scanner для Unix-систем 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, шпионского и рекламного ПО, а также "троянских коней", способных скомпрометировать целостность сети.

СИСТЕМНЫЕ ТРЕБОВАНИЯ

В целях обеспечения совместимости со всеми основными платформами на основе Unix-систем решения BitDefender для Unix-систем поставляются в виде пакетов rpm, deb и универсальных пакетов .tar.run.

Операционная система: Linux, FreeBSD, Linux Kernel: 2.4.x или 2.6.x (рекомендуется), FreeBSD: 5.4 (или более поздней версии с поддержкой библиотек compat5x)
glibc: версии 2.3.1 или более поздней версии, libstdc++5 из gcc 3.2.2 или более поздней версии
Процессор:

- архитектура x86, 300 МГц;
- i686 500 МГц;
- amd64(x86_64)

Минимальные требования к памяти: 128 МБ
Минимальное свободное пространство на диске: 100 МБ
Поддерживаемые дистрибутивы:

- RedHat Enterprise Linux 3 или более поздней версии
- SuSE Linux Enterprise Server 9 или более поздней версии
- Fedora Core 1 или более поздней версии
- Debian GNU/Linux 3.1 или более поздней версии
- Slackware 9.x или более поздней версии
- Mandrake/Mandriva 9.1 или более поздней версии
- FreeBSD 5.4 или более поздней версии

Проактивная защита

BitDefender Антивирус Scanner для Unix-систем обеспечивает защиту конечных точек для рабочих станций на основе Unix-систем

ПРОФИЛАКТИЧЕСКАЯ ЗАЩИТА КОНЕЧНЫХ ТОЧЕК

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. BitDefender Антивирус Scanner для Unix-систем включает в себя:

Защита от вирусов — помимо распознавания на основе сигнатур, продукты BitDefender предоставляют технологию эвристического распознавания и анализа, при использовании которой создается эмуляция виртуального "компьютера в компьютере", после чего все файлы и код проверяются на предмет вредоносного поведения. Данная технология обеспечивает более низкий коэффициент ложно-положительного обнаружения и значительно более высокий уровень распознавания для новых и неизвестных угроз.

Защита от шпионских программ Используя многоуровневый подход, BitDefender Антивирус Scanner для Unix-систем распознает известные шпионские и рекламные программы, что позволяет предотвратить утечку исходящих данных.

"Троянские кони" и руткиты: служат для обеспечения удаленного доступа 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.

Антивирусный сканер BitDefender использует не только списки известных сигнатур вирусов, но и технологии эвристического распознавания и анализа, которые поддерживают эмуляцию виртуального "компьютера в компьютере" и определяют вредоносный характер файлов и кода по их поведению. Данная технология отличается меньшим процентом ложных обнаружений и значительно более высоким уровнем распознавания новых и неизвестных угроз.

СКАНИРОВАНИЕ АРХИВОВ

BitDefender Антивирус Scanner для UNIX-систем способен распаковывать и сканировать архивы. Статус сканирования для отдельных файлов позволяет отслеживать выполнение сканирования для каждого архивированного файла. Для предотвращения активации эксплойтов (например, ZIP-бомб) введено ограничение глубины рекурсии архива. Администраторы также должны обращать внимание на любые файлы с многократным рекурсивным архивированием. Функциональные возможности BitDefender включают встроенную поддержку свыше 80 форматов упакованных файлов, включая архивы в формате RAR, ZIP, ARJ, LZH, LHA, ACE, GZIP, TARGZ, JAR, UUE, MIME или CAB, независимо от способа их создания (самораспаковывающиеся, многотомные и т. д.).

СКАНИРОВАНИЕ ПОЧТОВОГО ЯЩИКА

BitDefender Антивирус Scanner для Unix-систем можно использовать для сканирования определенных сообщений электронной почты или всего почтового ящика. При сканировании почтового ящика выполняется обнаружение сообщений, содержащих вложения, а также сканирование вложений каждого из сообщений. Для сценариев и расширений также предусмотрена интеграция с почтовыми клиентами (например, Pine, Evolution) и службами почтового сервера.

КАРАНТИН И ОТПРАВКА ВИРУСА ДЛЯ ИЗУЧЕНИЯ

В целях минимизации риска последующего заражения и выполнения безопасного анализа BitDefender Антивирус Scanner для UNIX-систем помещает инфицированные файлы в карантин в защищенном каталоге. Помимо инфицированных файлов в карантин могут помещаться также подозрительные файлы, в которых эвристический анализ обнаруживает определенные характеристики вредоносного кода, но при этом такие файлы не соответствуют известным вирусным сигнатурам. Инфицированные и подозрительные файлы анализируются локально, либо направляются в антивирусную лабораторию BitDefender для дальнейшего исследования.

ОБНОВЛЕНИЯ ПО ГРАФИКУ ПОСРЕДСТВОМ СЛУЖЕБНЫХ ПРОГРАММ

BitDefender Антивирус Scanner для Unix-систем можно настроить для автоматического обновления продуктов и вирусных сигнатур через Интернет. Если автоматические обновления не настроены, обновление можно в любой момент запустить вручную из графического пользовательского интерфейса или из командной строки.

Bitdefender