# McAfee Host Intrusion Prevention for Server

## Передовое средство защиты серверов и приложений от уязвимостей

Корпоративные серверы являются местом хранения самых ценных информационных активов любой организации и обеспечивают непрерывность ее работы. Одной из основных задач, стоящих перед ИТ, является обеспечение надежной защиты этих серверов и размещенных на них приложений от известных и неизвестных атак, угрожающих нарушить нормальный ход работы организации.

### McAfee Host Intrusion Prevention for Server

McAfee® Host Intrusion Prevention for Server представляет собой специализированное средство защиты веб-серверов и серверов баз данных, позволяющее поддерживать работоспособность систем и обеспечивать непрерывность работы организации. В него включен единственный в отрасли динамический брандмауэр, имеющий функцию отслеживания состояния соединений и обеспечивающий защиту от сложных угроз и вредоносного трафика. Кроме того, данное решение является системой предотвращения вторжений (IPS), работающей на основе сигнатур и анализа поведения. McAfee Host Intrusion Prevention for Server снижает срочность и частоту установки исправлений, поддерживает непрерывность ведения бизнеса и производительность труда сотрудников, защищает конфиденциальность данных и упрощает обеспечение соответствия нормативным требованиям.

### Защита серверов и приложения от атак, предотвращение утечки данных

Причиной растущего количества атак на серверы является тот факт, что на серверах хранятся большие объемы корпоративных данных и что серверам отводится критически важная роль в деле выполнения повседневных операций. McAfee Host Intrusion Prevention for Server обеспечивает защиту критически важных серверов, что позволяет поддерживать необходимый уровень бесперебойности и производительности в работе систем.

- Защита веб-серверов:
  - Фильтрация HTTP-запросов для предотвращения атак с целью прохождения каталогов, Unicode-атак и атак типа «отказ в обслуживании» (DoS)
  - Использование заранее определенных защищенных политик и правил, позволяющих предотвращать атаки и утечку данных

### Ключевые преимущества

**Усиленная защита**

- Обеспечьте широчайшую защиту от вторжений и угроз «нулевого дня» на всех уровнях, включая сети, приложения и системы.

**Снижение расходов**

- Снижайте трудоемкость и затраты с помощью единой мощной унифицированной консоли для развертывания, управления, составления отчетности и аудита событий, политик и агентов.
- Снижайте частоту и степень срочности установки исправлений на конечных точках.

**Упрощение процесса обеспечения нормативно-правового соответствия**

- Управляйте соответствием с помощью легких для восприятия и эффективных представлений, рабочих процессов, мониторинга событий и отчетности для проведения быстрых и надлежащим образом организованных расследований и разбирательств.

- Защита серверов баз данных:
  - Проверка запросов к базе данных для предотвращения атак, таких как «внедрение SQL»
  - Использование заранее определенных защищенных политик и правил, обеспечивающих стандартное поведение и предотвращающих умышленное изменение данных

### Передовая защита от угроз с помощью динамичного системного межсетевого экрана для рабочих станций с отслеживанием состояния соединений

В отличие от традиционных системных брандмауэров, работающих на основе определенных правил, McAfee Host Intrusion Prevention for Server подключен к системе McAfee Global Threat Intelligence (McAfee GTI) и получает информацию о репутации сетевых подключений, позволяющую в упреждающем режиме защищать серверы от таких сложных угроз, как бот-сети, атаки типа «распределенный отказ в обслуживании» (DDoS) и вредоносный трафик. В условиях роста количества сложных угроз безопасности именно McAfee GTI позволяет реализовать самый продуманный подход к обеспечению защиты.

### Менее частая и менее срочная установка исправлений операционных систем и приложений, причем — по собственному графику

Огромная доля средств использования уязвимостей выпускается в свет всего за три дня с момента выявления уязвимости. Многим организациям требуется порой до 30 дней на тестирование и установку всех исправлений для конечных точек.

McAfee Host Intrusion Prevention for Server сокращает разрыв в обеспечении безопасности, делая при этом процесс установки исправлений более легким и более ффективным.

- Серверы оказываются защищены и от уязвимостей Microsoft, и от уязвимостей Adobe. Функция экранирования уязвимостей автоматически обновляет сигнатуры, обеспечивая тем самым защиту конечных точек от атак, возникающих в результате использования уязвимостей.
- Регулярная автоматическая загрузка обновлений сигнатур позволяет обеспечить надежность защиты.

## Требования к системе

**Минимальные требования к аппаратному обеспечению**

- Intel или AMD x86 и x64
- Свободное место на диске (клиент): 15 МБ, но во время установки необходимо 100 МБ
- Память: 256 МБ ОЗУ
- Сетевое окружение: сети Microsoft или Novell NetWare; в случае NetWare сеть должна поддерживать TCP/IP
- Сетевая интерфейсная карта: сетевая интерфейсная карта; 10 Мбит/с или больше

**Поддерживаемые операционные системы**

- Microsoft Windows Server 2003 SP2, 2003 R2, 2003 R2 SP2 (все выпуски, 32- и 64-разрядные)
- Microsoft Windows Server 2008, 2008 SP1, 2008 SP2, 2008 R2 (все выпуски, 32- и 64-разрядные)
- SPARC Solaris 9 sun4u (32- и 64-разрядные версии)
- SPARC Solaris 10 sun4u, sun4v (32- и 64-разрядные версии)
- Red Hat Linux Enterprise 4 (32-разрядная версия)
  - 2.6.9-5.EL
  - 2.6.9-5.Elhugemem
  - 2.6.9-5.ELsmp

## Положен конец уязвимостям серверов во время запуска

Только что запущенный сервер является уязвимым до тех пор, пока не будут применены политики безопасности. Во время запуска сервер может подвергнуться сетевой атаке, на нем могут быть отключены защитные службы. McAfee Host Intrusion Prevention for Server блокирует атаки, способные произойти во время этого уязвимого промежутка времени, с помощью специальных функций брандмауэра и системы IPS, активируемых на время их запуска.

- Функция защиты запуска брандмауэра, активируемая во время запуска компьютера (т. е. до полной активации всей политики брандмауэра), пропускает только исходящий трафик.
- Функция защиты IPS, активируемая во время запуска компьютера (т. е. до полной активации всей политики IPS), предотвращает отключение наших защитных служб.

## Упрощение и упорядочение процессов управления

Крупные организации не могут обойтись без создания и редактирования большого количества разных политик брандмауэра и системы предотвращения вторжений (IPS), но этот процесс, как правило, отнимает у сотрудников большое количество сил и времени. Для упорядочения данного процесса в McAfee Host Intrusion Prevention for Server используются каталоги политик и IPS, позволяющие создавать и редактировать большое количество разных политик брандмауэра и IPS, чтобы затем применять их по мере необходимости.

Еще больше оптимизировать и упростить процессы управления позволяет программное обеспечение McAfee® ePolicy Orchestrator® (McAfee ePO™) — наша единая, централизованная консоль управления, помогающая контролировать и администрировать все средства защиты. Полная интеграция с программным обеспечением McAfee ePO позволяет экономить время и деньги и повышает эффективность работы.

Для получения дополнительной информации свяжитесь с нашим представителем или посетите наш веб-сайт по адресу **www.mcafee.com/ru**.

## Требования к системе (продолжение)

**Поддерживаемые операционные системы (продолжение)**

- Red Hat Linux Enterprise 4 (64-разрядная версия)
  - 2.6.9-5.EL
  - 2.6.9-5.ELsmp
- Red Hat Linux Enterprise 5 (32-разрядная версия)
  - 2.6.18-8.el5
  - 2.6.18-8.el5PAE
- Red Hat Linux Enterprise 5 (64-разрядная версия)
  - 2.6.18-8.el5
- SUSE Linux Enterprise 10 (32-разрядная версия)
  - 2.6.16.21-0.8-bigsmp
  - 2.6.16.21-0.8-default
  - 2.6.16.21-0.8-smp
- SUSE Linux Enterprise 10 (64-разрядная версия)
  - 2.6.16.21-0.8-default
  - 2.6.16.21-0.8-smp
- SUSE Linux Enterprise 11 (32-разрядная версия)
  - 2.6.27.19-5-default
  - 2.6.27.19-5-pae
- SUSE Linux Enterprise 11 (64-разрядная версия)
  - 2.6.27.19-5-default

## Совместимость с основными платформами виртуализации

На сегодняшний день технологии виртуализации используются в ИТ-подразделениях практически всех организаций, поэтому совместимость с основными платформами виртуализации является обязательным условием успеха любого продукта. Решение McAfee Host Intrusion Prevention for Server 8.0 совместимо с тремя основными платформами виртуализации: VMware, Citrix и Microsoft Hyper-V. В приведенной ниже таблице перечислены поддерживаемые продукты этих трех поставщиков.

| VMware | Citrix | Microsoft |
|---|---|---|
| VMware ESX 3.5 и 4.0 | Citrix XenServer 5.0 и 5.5 | Microsoft Hyper-V Server 2008 и 2008 R2 |
| VMware Vsphere 4.0 | Citrix XenDesktop 3.0 и 4.0 | Microsoft VDI |
| VMware View 3.1 и 4.0 | Citrix XenApp 5.0 и 6.0 | Microsoft App-V 4.5 и 4.6 |
| VMware ThinApp 4.0 и 4.5 | | Режим XP в Windows 7 |
| VMware ACE 2.5 и 2.6 | | |
| VMware Workstation 6.5 и 7.0 | | |
| VMware Player 2.5 и 3.0 | | |

## Требования к системе (продолжение)

**Поддерживаемые веб-серверы**

- Microsoft Windows
  - IIS 6.0 и 7.0
- SPARC Solaris
  - Apache 1.3.6 и веб-сервер более поздней версии
  - Apache 2.0.42 и веб-сервер более поздней версии
  - Apache 2.2.3 и веб-сервер более поздней версии
  - Sun Java Web Server 6.1
  - Sun Java Web Server 7.0
- Linux (RHEL и SUSE)
  - Apache 1.3.6 и веб-сервер более поздней версии
  - Apache 2.0.42 и веб-сервер более поздней версии
  - Apache 2.2.3 и веб-сервер более поздней версии

**Поддерживаемые серверы баз данных**

- Microsoft SQL Server 2005 и 2008

McAfee Together is power.

McAfee Ireland Ltd.
Building 2000, City Gate
Mahon, Cork, Ireland
www.mcafee.com/ru