



McAfee Host Intrusion Prevention for Desktop

Передовое средство защиты настольных компьютеров и ноутбуков от уязвимостей

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.

Поскольку количество киберпреступников, движимых жаждой наживы, непрерывно растет, а исходящие от них угрозы безопасности имеют сложный и изощренный характер, управление безопасностью и контроль сетевых подключений на настольных и портативных компьютерах в масштабах целой организации становится все более и более сложной задачей. По мере увеличения степени мобильности персонала на ИТ-подразделения ложится дополнительная ответственность по обеспечению безопасности подключения пользователей к корпоративной сети. Кроме того, организациям нужны средства защиты от угроз «нулевого дня», позволяющие выигрывать время, требуемое для надлежащей приоритизации, тестирования и развертывания необходимых исправлений.

Задача

Уже невозможно обеспечить достаточную защиту с помощью одной лишь антивирусной программы, так как атаки и средства использования уязвимостей, появляются все быстрее и становятся все более сложными. Решение этой проблемы состоит в реализации упреждающей стратегии безопасности, в первую очередь предотвращающей выполнение атаки. Используя упреждающий подход к защите конечных точек, ИТ-подразделения могут гарантировать, что все конечные точки и конфиденциальные данные защищены, а непрерывной работе бизнеса ничто не может помешать.

McAfee Host Intrusion Prevention for Desktop

Являясь неотъемлемой частью наших комплектов решений для защиты конечных точек, McAfee® Host Intrusion Prevention for Desktop обеспечивает беспрецедентный уровень защиты от известных и неизвестных угроз «нулевого дня» благодаря сочетанию системы предотвращения вторжений (IPS) на основе сигнатур и анализа поведения с единственным в отрасли динамическим брандмауэром, имеющим функцию отслеживания состояния соединений. McAfee Host Intrusion Prevention for Desktop снижает срочность и частоту установки исправлений, поддерживает непрерывность ведения бизнеса и производительность труда сотрудников, защищает конфиденциальность данных и упрощает обеспечение соответствия нормативным требованиям.

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: 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 XP SP2, SP3 (только 32-разрядная версия)

- Professional Edition

Microsoft Windows Vista, Vista с SP1 (32- и 64-разрядные версии)

- Business Edition
- Enterprise Edition
- Ultimate Edition

Microsoft Windows 7 (32- и 64-разрядные версии)

- Professional Edition
- Enterprise Edition
- Ultimate Edition

Передовая защита от угроз с помощью динамичного брандмауэра для рабочих станций с отслеживанием состояния соединений

В отличие от традиционных системных брандмауэров, работающих на основе определенных правил, McAfee Host Intrusion Prevention for Desktop подключен к системе McAfee Global Threat Intelligence (McAfee GTI) и получает информацию о репутации сетевых подключений, позволяющую в упреждающем режиме защищать настольные и портативные компьютеры 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. Наличие таких дополнительных функций брандмауэра, как блокирование трафика в зависимости от используемого приложения или местонахождения пользователя, позволяет повысить надежность защиты ноутбуков и настольных компьютеров особенно в случае их нахождения за пределами корпоративной сети.

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 Desktop сокращает разрыв в обеспечении безопасности, делая при этом процесс установки исправлений более легким и более эффективным.

- McAfee Host Intrusion Prevention for Desktop обеспечивает защиту от большинства современных средств использования уязвимостей. Пользователь получает защиту как от уязвимостей Microsoft, так 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.

Положен конец уязвимостям конечных точек во время запуска

Только что запущенный ноутбук или настольный компьютер является уязвимым до тех пор, пока не будут применены политики безопасности. Во время запуска конечные точки могут подвергнуться сетевой атаке, на них могут быть отключены защитные службы. McAfee Host Intrusion Prevention for Desktop блокирует атаки, способные произойти во время этого уязвимогo промежутка времени, с помощью специальных функций брандмауэра и системы предотвращения вторжений (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 IPS, но этот процесс, как правило, отнимает у сотрудников большое количество сил и времени. Для упорядочения данного процесса в McAfee Host Intrusion Prevention for Desktop используются каталоги политик и IPS, позволяющие создавать и редактировать большое количество разных политик брандмауэра и IPS, которые можно применять к разным группам пользователей и при необходимости использовать повторно.

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.ru.

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 Desktop 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 ESXi 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		



McAfee. Part of Intel Security.

Адрес: Москва, Россия, 123317
Пресненская набережная, 10
БЦ «Башни на набережной»,
Башня «А», 15 этаж
Телефон: +7 (495) 653-85-13
www.intelsecurity.com

Intel, логотипы Intel и McAfee, ePolicy Orchestrator и McAfee ePO являются товарными знаками Intel Corporation или McAfee, Inc. в США и/или других странах. Другие названия и фирменная символика являются собственностью соответствующих владельцев. Copyright © 2010 McAfee, Inc. 17801ds_hips-desktop_1110B