

# McAfee Host Intrusion Prevention for Desktop

## Передовое средство защиты настольных компьютеров и ноутбуков от уязвимостей

Поскольку количество киберпреступников, движимых жадой 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 комплектов решений McAfee® для защиты конечных точек, McAfee Host Intrusion Prevention for Desktop обеспечивает непревзойденный уровень защиты от известных и неизвестных угроз «нулевого дня» благодаря сочетанию системы предотвращения вторжений (IPS) на основе сигнатур и анализа поведения с динамическим брандмауэром, имеющим функцию отслеживания состояния соединений. McAfee Host Intrusion Prevention for Desktop снижает срочность и частоту установки исправлений, поддерживает непрерывность ведения бизнеса

### 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 позволяющих принимать конкретные меры представлений, рабочих процессов, мониторинга событий и отчетности для проведения быстрых и надлежащим образом организованных расследований и компьютерно-технических экспертиз.

и производительность труда сотрудников, защищает конфиденциальность данных и упрощает обеспечение соответствия нормативным требованиям.

### **Передовая защита от угроз с помощью динамического 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 одну из самых продуманных услуг обеспечения 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**

Большая доля средств использования уязвимостей выпускается уже через три дня после выявления уязвимости, и все же многим организациям требуется порой до 30 дней на тестирование и установку исправлений для всех конечных точек. McAfee Host Intrusion Prevention for Desktop сокращает разрыв в обеспечении безопасности, делая при этом процесс установки исправлений более легким и эффективным.

- McAfee Host Intrusion Prevention for Desktop обеспечивает защиту от атак «нулевого дня» и неустранимых 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.

### **Требования к системе**

---

#### **Поддерживаемые операционные системы**

- Microsoft Windows Server 10
- Microsoft Windows Server 8.1
- Microsoft Windows Server 8
- Microsoft Windows 7 с SP1 (32- и 64-разрядные версии): Business, Enterprise, Ultimate
- Microsoft Windows Embedded Standard 7 с SP1 (32- и 64-разрядные версии)
- Microsoft Windows Vista (32- и 64-разрядные версии): Business, Enterprise, Ultimate
- Microsoft Windows XP Professional (32-разрядная версия)
- Windows XP Professional for Embedded Systems (32-разрядная версия)
- Microsoft Windows Embedded (32-разрядная версия)

### 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 уязвимого 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 много сил и времени. Для упорядочения данного процесса в McAfee Host Intrusion Prevention for Desktop используются каталоги политик и IPS, позволяющие создавать и редактировать множество 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.

### Совместимость с основными платформами виртуализации

Виртуализация позволяет сократить расходы, увеличить гибкость и упростить обслуживание продуктов. Решение McAfee Host Intrusion Prevention for Desktop совместимо с разными основными платформами виртуализации: VMware, Citrix и Microsoft.

Для получения дополнительной информации посетите страницу [www.mcafee.com/ru/products/host-ips-for-desktop.aspx](http://www.mcafee.com/ru/products/host-ips-for-desktop.aspx).

### Требования к системе

#### Поддерживаемые системы виртуализации

- Citrix XenServer: 5.0, 5.5
- Citrix XenDesktop: 3.0, 4.0, 7.5, 7.6
- Citrix XenApp: 5.0, 6.0, 6.5
- Citrix Provisioning Services 6.1
- Microsoft App-V: 4.5, 4.6
- Microsoft Hyper-V Server: 2008, 2008 R2
- Microsoft Windows Server: 2008, Hyper-V 2008, 2008 R2, 2012 R2
- Microsoft VDI (пакет)
- MED-V: 1.0, 1.0 SP1
- SCVMM: 2008, 2008 R2
- SCCM: 2007 SP2, 2007 R2
- SCOM: 2007, 2007 R2
- VMware ACE: 2.5, 2.6
- VMware ESX: 3.5, 4.0, 5.0
- VMware ESXi 5.1
- VMware Player: 2.5, 3.0, 5.0
- VMware Server: 1.0, 2.0
- VMware Thin App: 4.0, 4.5
- VMware Vsphere 4.0
- VMware View: 4 3.1, 4.0
- VMware Workstation: 6.5, 7.0, 8.0, 9.0
- Режим XP в Windows 7: 32- и 64-разрядные версии



McAfee Ireland Ltd.  
Building 2000, City Gate  
Mahon, Cork, Ireland  
[www.mcafee.com/ru](http://www.mcafee.com/ru)

McAfee и логотип McAfee являются товарными знаками или зарегистрированными товарными знаками компании McAfee, LLC или ее филиалов в США и других странах. Другие названия и фирменная символика являются собственностью соответствующих владельцев. Copyright © 2017 McAfee, LLC. 62140\_1015 Октябрь 2015 г.