McAfee Host Intrusion Prevention для серверов

Проактивная защита серверов и приложений

Основные преимущества

Усиленная защита

- Реализует широкомасштабную защиту от вторжений и угроз нулевого дня на серверах для всех уровней: уровня сети, приложения и выполнения кода

Более низкие расходы

- С помощью единой мощной унифицированной консоли для развертывания, управления, составления отчетности и аудита событий, политик и агентов сокращается трудоемкость и затраты
- Исправления устанавливаются на сервер менее часто и не столь срочно

Упрощается обеспечение соответствия нормативным требованиям

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

Проблема

Ваши корпоративные серверы хранят наиболее ценные информационные активы и поддерживают жизнеспособность вашего бизнеса. Для менеджера ИТ одной из сложнейших производственных задач является успешная защита этих серверов и приложений от известных и неизвестных атак, которые грозят прерыванием бизнеса. Для реализации этой цели необходимо развернуть технологии безопасности по всей сети предприятия.

При этом сложность вредоносных программ, нацеленных на уязвимости ваших серверов и приложений, непрерывно возрастает в такой же пропорции, что и защита. В первой половине января 2008 года появилось больше новых угроз, чем за весь 2007 год.[1] Если учесть, что более 32 процентов[2] вредоносных программ появлялось в течение трех дней с момента выявления уязвимости, организации подвергаются большому риску, поскольку на развертывание исправлений на серверах предприятия в среднем требуется 32 дня.[3] Вам необходима защита от угроз нулевого дня, чтобы обеспечить безопасность ИТ и предоставить время на приоритизацию, планирование, тестирование и развертывание исправлений. Ключ к выигрышу в этой игре — реализация проактивной стратегии безопасности, в первую очередь предотвращающей выполнение атаки. Используя проактивный подход к защите серверов и приложений, вы можете оставаться уверенными в том, что ваши конфиденциальные данные защищены, а непрерывной работе бизнеса ничто не может помешать.

McAfee Host Intrusion Prevention для серверов

McAfee® Host Intrusion Prevention (Host IPS) осуществляет мониторинг и блокирует нежелательные действия и угрозы. Серверная версия Host IPS обеспечивает бесперебойную работу сервера и защищает корпоративные активы, такие как приложения и базы данных. Host IPS защищает серверы как от известных, так и от неизвестных угроз нулевого дня, объединяя предотвращение вторжения на основе анализа поведения и сигнатур с межсетевым экраном и контролем приложений. McAfee Host IPS снижает срочность и частоту установки исправлений, сохраняет бесперебойность работы бизнеса и производительность сотрудников, защищает конфиденциальность данных и упрощает обеспечение соответствия нормативным требованиям.

Легкость управления в масштабах предприятия

McAfee ePolicy Orchestrator® (ePO™) — самая передовая в отрасли платформа управления безопасностью, которая обеспечивает скоординированную упреждающую защиту предприятия от угроз, связанных с вредоносными программами и атаками. С помощью консоли ePO, представляющей собой центральный пункт для решений McAfee, выполняется управление рисками в системе безопасности, администраторы могут обеспечивать актуальность защиты, настраивать и внедрять политики защиты, а также круглосуточно и ежедневно отслеживать состояние защиты с одной централизованной консоли на основе веб-приложения. Разверните платформу ePO и управляйте всеми новыми решениями для безопасности, либо наращивайте объем средств, вложенных в управление безопасностью предприятия, добавив к инфраструктуре ePO решение Host IPS. При наличии ePO, Host IPS легко развертывается, настраивается и не вызывает трудностей в управлении.

1 McAfee Labs™

2 McAfee Labs™

3 Forrester: The State of Server Operating System Security 2007—Administrators Patch an Average of Eight Days Late, June 2007 («Состояние безопасности операционных систем серверов 2007 — администраторы устанавливают пакеты исправлений в среднем на восемь дней позже»), июнь 2007 года

Системные требования

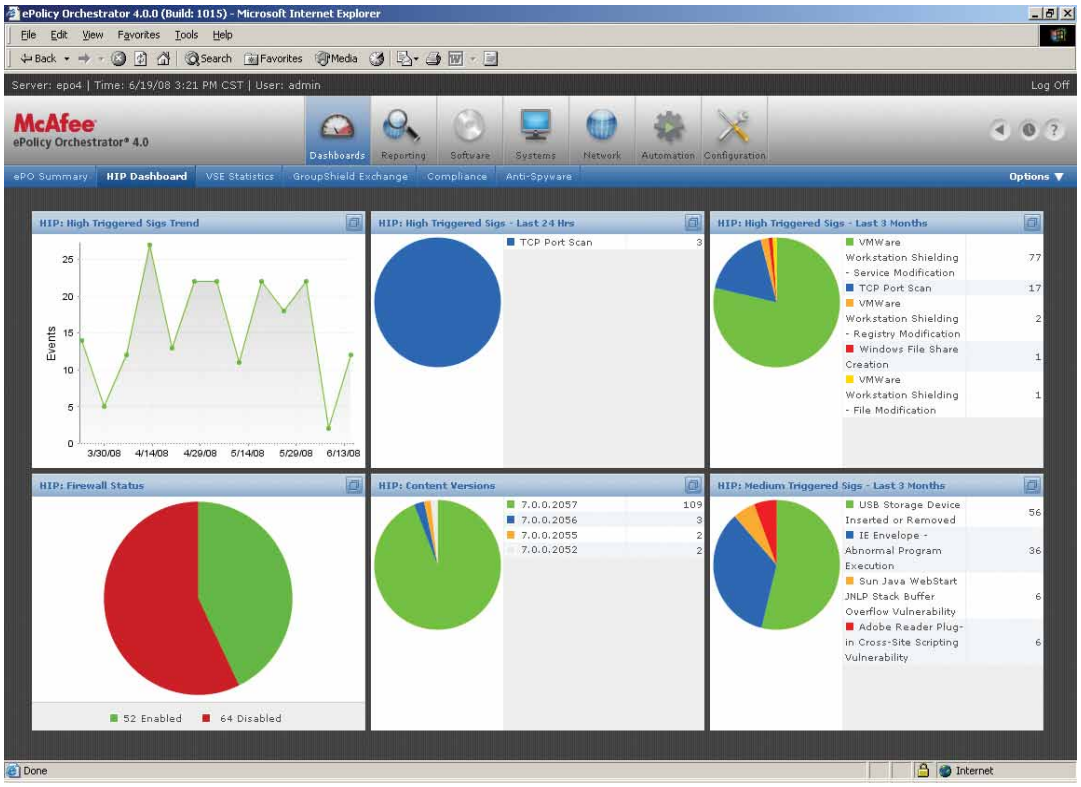
- Microsoft Windows (английская, французская, немецкая, испанская, японская, корейская и традиционная китайская версии)
- Microsoft Windows 2000 Advanced Server с пакетом обновления 3 или более поздней версии
- Microsoft Windows 2000 Datacenter Server с пакетом обновления 3 или более поздней версии
- Microsoft Windows 2000 Professional с пакетом обновления 3 или более поздней версии
- Microsoft Windows 2000 Server с пакетом обновления 3 или более поздней версии
- Microsoft Windows Server 2003 Enterprise с пакетом обновления 2 или более поздней версии, 32- и 64-разрядная версии
- Microsoft Windows Server 2003 R2 Enterprise, 32- и 64-разрядная версии
- Microsoft Windows Server 2003 Standard с пакетом обновления 2, 32- и 64-разрядная версии
- Microsoft Windows Server 2003 R2 Standard, 32- и 64-разрядная версии
- Microsoft Windows Server 2003 Web с пакетом обновления 1 или более поздней версии
- Microsoft Windows Server 2003 R2 Web
- Microsoft Windows Server 2008

Возможности и преимущества

Многоуровневая защита обеспечивает широкий и комплексный охват активов

При быстром росте смешанных угроз и ориентированной на получение прибылей киберпреступности, предприятиям необходима многоуровневая безопасность для защиты конечных точек от известных и неизвестных угроз нулевого дня с целью предотвращения утечки конфиденциальных данных.

- **Защита, основанная на сигнатурах,** точно определяет и блокирует известные атаки
- **Защита, основанная на поведении,** защищает конечные точки от новых угроз нулевого дня, таких как атаки, вызывающие переполнение буфера
- **Межсетевой экран, отслеживающий состояние соединений,** блокирует нежелательный входящий трафик, контролирует исходящий трафик и применяет правила политик, основанные на трафике, портах, приложениях и объектах их применения
- **Контроль приложений** помогает в создании белых и черных списков, в которых указывается, какие приложения могут или не могут выполняться
- **Специализированная защита сервера** обеспечивает безопасность критически важных серверов с помощью адаптированных пользователем средств защиты для поддержания бесперебойной работы системы и производительности труда пользователей
  - Веб-сервер
    - » Фильтрация HTTP-запросов для предотвращения атак с целью прохождения каталогов, Unicode-атак и атак типа «отказ в обслуживании»
    - » Использование заранее определенных защищенных политик и правил, позволяющих предотвращать атаки и утечку данных
  - Сервер базы 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



Панели мониторинга ePO делают просмотр данных Host IPS легким и понятным.

Системные требования (продолж.)

Red Hat Enterprise Linux 4.0 (только 32-разрядная версия)
Поддерживаются приведенные ниже модули ядра Red Hat Enterprise Linux 4:
- 2.6.9-22.EL
- 2.6.9-22.EL-smp
- 2.6.9-34.EL
- 2.6.9-34.EL-smp
- 2.6.9-42.EL
- 2.6.9-42.EL-smp

Sun Solaris
- SPARC Solaris 8 (32- или 64-разрядное ядро)
- SPARC Solaris 9 (32- или 64-разрядное ядро)
- SPARC Solaris 10

Поддерживаемые платформы веб-серверов
- IIS 4.0, 5.0 и 6.0 (Microsoft Windows)
- Apache 1.3.6 и веб-сервер боле поздней версии
- Apache 2.0.42 и веб-сервер боле поздней версии
- Sun ONE Web Server 6.0
- Sun Java System Web Server 6.1

Поддерживаемые платформы серверов баз данных
- Microsoft SQL Server 2000 (Windows) SP3a, SP4

Ваше ИТ-подразделение будет реже и не столь срочно устанавливать исправления, причем по собственному графику

Огромная доля вредоносных программ выпускается в свет всего за три дня с момента выявления уязвимости. В среднем же предприятиям требуется 32 дня для развертывания исправлений на серверах. Host IPS сокращает разрыв в обеспечении безопасности, делая при этом процесс установки исправлений более легким и более эффективным.

- **Закрытие уязвимостей** автоматически обновляет сигнатуры для защиты конечных точек от атак, являющихся результатом использования уязвимости
- **Готовое к работе решение,** обеспечивающее наилучшие результаты: Host IPS защитило 97 процентов[4] всех уязвимостей Microsoft, обнаруженных в 2007 году
- **Обновления сигнатур** автоматически и регулярно загружаются таким же образом, как и обновления на основе файлов .DAT, чтобы гарантировать актуальность защиты

Платформа ePO консолидирует и централизует управление всеми продуктами McAfee

Компании борются за снижение затрат и усилий, необходимых для управления отдельными технологиями безопасности, развернутыми на их конечных точках и в сети. Используя единую интегрированную консоль управления, компании на 44 процента сокращают штат ИТ-менеджеров, по сравнению с их численностью, необходимой для управления безопасностью конечных точек с помощью нескольких консолей.[5]

- Получите доступ к централизованному мониторингу событий, отчетам, панели мониторинга и последовательностям выполнения работ посредством единой консоли
- Развертывайте, управляйте и обновляйте агентов и политику, пользуясь одной платформой управления

Затрачивайте меньше времени на сбор данных, необходимых для достижения и подтверждения соответствия, а также для подготовки отчетности

Поддержание соответствия нормативным требованиям и его подтверждение могут поглощать неимоверное количество ИТ-ресурсов. Host IPS помогает предприятиям достичь лучших возможностей просмотра событий и усовершенствовать управление, упростив и сделав менее болезненным процесс обеспечения соответствия, подготовки отчетов и проведения аудитов.

- Собирайте сведения об атаках, такие как тип, направление, источник, серьезность, временная метка и прочее, в ясном и простом для понимания виде для быстрого уведомления, проведения аудита, расследования и принятия ответных мер.
- Генерируйте отчеты о соответствии для аудиторов и других заинтересованных лиц.
- Настраивайте панели мониторинга для отображения статуса соответствия в реальном времени.

4 McAfee Labs™
5 Insight Express, 2007

ООО «МакАфи Рус»
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
Бизнес центр «Башни на набережной»
4ый этаж, офис 405 – 409
Телефон: +7 (495) 967 76 20
Факс: +7 (495) 967 76 00
www.McAfee.ru

9731ds_hips-server_0710_fnl