CA Host-Based Intrusion Prevention System r8.1

ПРОГРАММНЫЙ ПАКЕТ CA HOST-BASED INTRUSION PREVENTION SYSTEM, HIPS (СЕРВЕРНАЯ СИСТЕМА ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ) ОБЪЕДИНЯЕТ АВТОНОМНЫЙ МЕЖСЕТЕВОЙ ЭКРАН И СИСТЕМУ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ В ЦЕНТРАЛИЗОВАННУЮ ПРОАКТИВНУЮ СИСТЕМУ ЗАЩИТЫ ОТ ИЗВЕСТНЫХ И НЕИЗВЕСТНЫХ СЕТЕВЫХ УГРОЗ. В ЭТОЙ СИСТЕМЕ ЗАЩИТНЫЙ МЕХАНИЗМ, ОСНОВАННЫЙ НА МОНИТОРИНГЕ ПОВЕДЕНИЯ, ДОПОЛНЯЕТ ТЕХНОЛОГИИ, ПОСТРОЕННЫЕ НА ОБНАРУЖЕНИИ СИГНАТУР ИЗВЕСТНЫХ УГРОЗ, В РЕЗУЛЬТАТЕ МЫ ПОЛУЧАЕМ ЭКСТРАОРДИНАРНУЮ ЗАЩИТУ, УПРАВЛЕНИЕ ДОСТУПОМ, УПРАВЛЕНИЕ ПРИНУДИТЕЛЬНЫМ ПРИМЕНЕНИЕМ ПОЛИТИК БЕЗОПАСНОСТИ И ПРЕДОТВРАЩЕНИЕМ ВТОРЖЕНИЙ ЧЕРЕЗ ЕДИНУЮ, ОБЛАДАЮЩУЮ ИНТУИТИВНО ПОНЯТНЫМ ИНТЕРФЕЙСОМ КОНСОЛЬ.

Обзор продукта

Вредоносный код и комбинированные угрозы развиваются слишком быстро, чтобы их можно было остановить при помощи традиционных средств и технологий защиты от угроз. Необходим комбинированный механизм защиты, который свяжет в многоуровневую систему все средства обеспечения безопасности конечной точки системы. CA HIPS объединяет автономный межсетевой экран и систему обнаружения и предотвращения вторжений, дополняя технологии защиты, построенные на обнаружении сигнатур известных угроз, централизованной проактивной защитой от известных и неизвестных угроз.

Достоинства

Добавляя к существующим средствам защиты от угроз программный пакет CA HIPS, вы расширяете систему защиты конечной точки за счет централизованного управления доступом и принудительного применения политик безопасности. Разнообразные известные и неизвестные угрозы эффективно блокируются, благодаря чему снижается риск простоев, сокращаются или устраняются расходы на устранение вреда и службу технической поддержки в виде «горячей линии».

Преимущества CA

CA HIPS дополняет другие продукты для управления защитой от угроз компании CA и, вместе с тем, предоставляет комплексную и многоуровневую систему защиты от известных и неизвестных угроз. Решения обеспечения безопасности от компании CA являются одним из фундаментальных компонентов более общей концепции этой компании - Enterprise IT Management, EITM (Управление ИТ на уровне организации), цель которой - унификация, упрощение и обеспечение безопасности информационных технологий.

МОСКВА, 119334, УЛ. БАРДИНА, Д. 4, КОРП. 1
ТЕЛ./ФАКС: +7 (495) 925-0049, (499) 135-2519
САНКТ-ПЕТЕРБУРГ, 192007, НАБ. ОБВОДНОГО КАНАЛА, Д. 64, СТР. 2
ТЕЛ./ФАКС: +7 (812) 337-1911, 337-1912

Программное обеспечение CA HIPS отвечает на комбинированные угрозы комбинированной системой защиты

Феномен вредоносного программного обеспечения эволюционировал из хакерского спорта, которым занимались любители похвастаться своими достижениями, в криминальную организацию, ряды которой пополняются специалистами по созданию программного обеспечения, алчущими нелегальных доходов. Такие авторы преступного ПО используют изощренные комбинации различных методов атак для компрометации программных продуктов, использующих традиционные технологии защиты от угроз, нацеливаясь на быстро растущий и все более разнообразный парк удаленных и мобильных конечных устройств и используя возможности, предоставляемые существованием «только что открытых» уязвимостей в программном обеспечении, так называемых «zero-day vulnerabilities».

Построенные на методиках обнаружения сигнатур угроз антивирусные и антишпионские продукты играют важную роль в обеспечении безопасности конечных устройств, но это методы реагирования, не предоставляющие защиты от провалов в системе безопасности, которые возникают в режиме реального времени и становятся особенно актуальными в связи с появлением комбинированных угроз и атак с использованием вновь обнаруженных уязвимостей, не учтенных в базах сигнатур угроз этих продуктов. Комбинированные угрозы требуют комбинированной и многоуровневой системы защиты, а для защиты от атак с использованием вновь обнаруженных уязвимостей, для которых пока не разработаны исправления безопасности, необходимы проактивные, построенные на мониторинге поведения, системы защиты.

CA HIPS создает эффективное решение защиты от угроз «3 в1», которое объединяет автономный межсетевой экран и средства обнаружения и предотвращения вторжений под централизованным, построенным на применении политик безопасности, управлением. Используя CA HIPS, вы можете вести мониторинг сетевого трафика и поведения системы и выявлять отклонения, которые зачастую свидетельствуют о новых угрозах.

Серверное программное обеспечение не прекращает защиту конечных точек даже тогда, когда они отключены от сети. Когда пользователь вновь подключается к сети, серверный компонент автоматически передает все новые обновления политик на его устройство.

CA HIPS скрывает сложный механизм управления политиками за интуитивно понятным интерфейсом. Вы можете строить политики безопасности на нескольких факторах – например, территориальном расположении пользователя, времени дня или роли отдельного пользователя в организации – и применять их динамически. Администраторы могут использовать тонко-гранулированные средства настройки политик и «режим обучения», чтобы адаптировать решение CA HIPS к способу, который принят в вашей организации для работы с программным обеспечением.

Основные функциональные возможности:

ТРИ МЕТОДА ЗАЩИТЫ ОТ УГРОЗ В ОДНОМ РЕШЕНИИ. Сочетание автономного межсетевого экрана и системы обнаружения и предотвращения вторжений формирует проактивную систему защиты конечной точки от известных и неизвестных угроз. Управление доступом, принудительное применение и развертывание политик безопасности осуществляется через консоль с интуитивно понятным Web-интерфейсом.

ЗАЩИТА В РЕАЛЬНОМ ВРЕМЕНИ НА ОСНОВЕ МОНИТОРИНГА ПОВЕДЕНИЯ CA HIPS ИМЕЕТ РЕЖИМ обучения, который можно использовать для создания на основе обычного поведения системы точки отсчета, в соответствии с которой будут создаваться и адаптироваться политики безопасности. В результате можно точно отрегулировать систему обнаружения аномалий и предотвратить ложные срабатывания, а также настроить защиту от угроз таким образом, чтобы она соответствовала потребностям бизнеса.

МОСКВА, 119334, УЛ. БАРДИНА, Д. 4, КОРП. 1
ТЕЛ./ФАКС: +7 (495) 925-0049, (499) 135-2519
САНКТ-ПЕТЕРБУРГ, 192007, НАБ. ОБВОДНОГО КАНАЛА, Д. 64, СТР. 2
ТЕЛ./ФАКС: +7 (812) 337-1911, 337-1912

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ ПОЛИТИКАМИ. Благодаря централизованному созданию, развертыванию и обслуживанию политик безопасности, постоянное администрирование политик безопасности во всей организации становится простым и конструктивным. Через интуитивно понятный графический интерфейс можно настраивать политики безопасности, которые будут применяться к группам пользователей, типам конечных устройств, функциям обеспечения безопасности и уровням безопасности.

ГРАНУЛЯРНОСТЬ В НАСТРОЙКЕ ПРАВИЛ И ПОЛИТИК БЕЗОПАСНОСТИ. Администраторы могут определять уровень доступа и контролировать его применительно к системам, группам пользователей или отдельным пользователям. Кроме того, они могут устанавливать политики, которые будут применяться к определенным пользователям в течение определенного времени суток или при выполнении ими определенных ролей в определенных местах.

КОМПЛЕКСНОЕ УПРАВЛЕНИЕ СОБЫТИЯМИ. Сервер CA HIPS ведет сбор и запись событий, происходящих на каждой клиентской машине, и предоставляет фильтры, которые администраторы могут использовать для просмотра только важных событий. Список критериев фильтрации предлагается в виде удобного раскрывающегося меню.

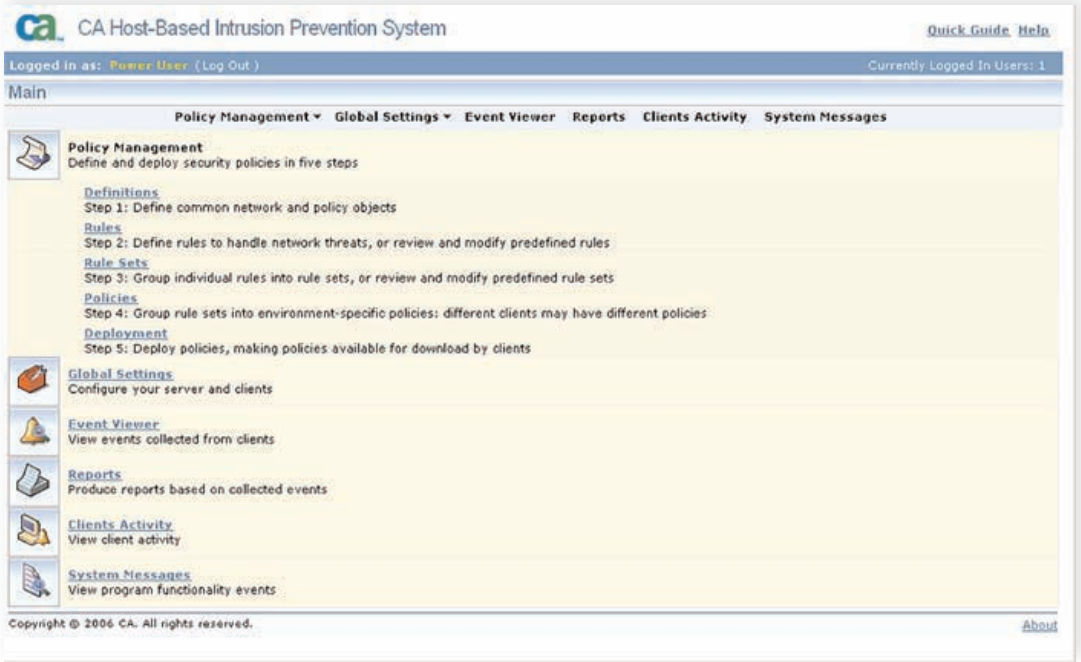
КЛИЕНТСКИЙ ИНТЕРФЕЙС ПОЛЬЗОВАТЕЛЯ НА ОСНОВЕ ПОЛИТИК БЕЗОПАСНОСТИ. CA HIPS предоставляет интуитивно понятный клиентский пользовательский интерфейс для конечного пользователя. В зависимости от установленных администратором политик конечный пользователь может видеть и изменять меры обеспечения безопасности для своего ПК, при необходимости блокируя новые атаки со своего рабочего места. Эта функция находится под централизованным контролем и может включаться или отключаться по решению администратора.

МНОГОЯЗЫЧНОСТЬ ДЛЯ ПОДДЕРЖКИ ГЛОБАЛЬНОГО РАЗВЕРТЫВАНИЯ. CA HIPS поддерживает английский, французский, итальянский, немецкий, упрощенный китайский, бразильский вариант португальского и испанский языки.

РИСУНОК А

ГЛАВНОЕ ОКНО АДМИНИСТРАТОРА

Главное окно CA HIPS позволяет управлять ПО CA HIPS в вашей среде. Администратор может создавать и развертывать политики и правила обеспечения безопасности на всех клиентских машинах CA HIPS в организации.

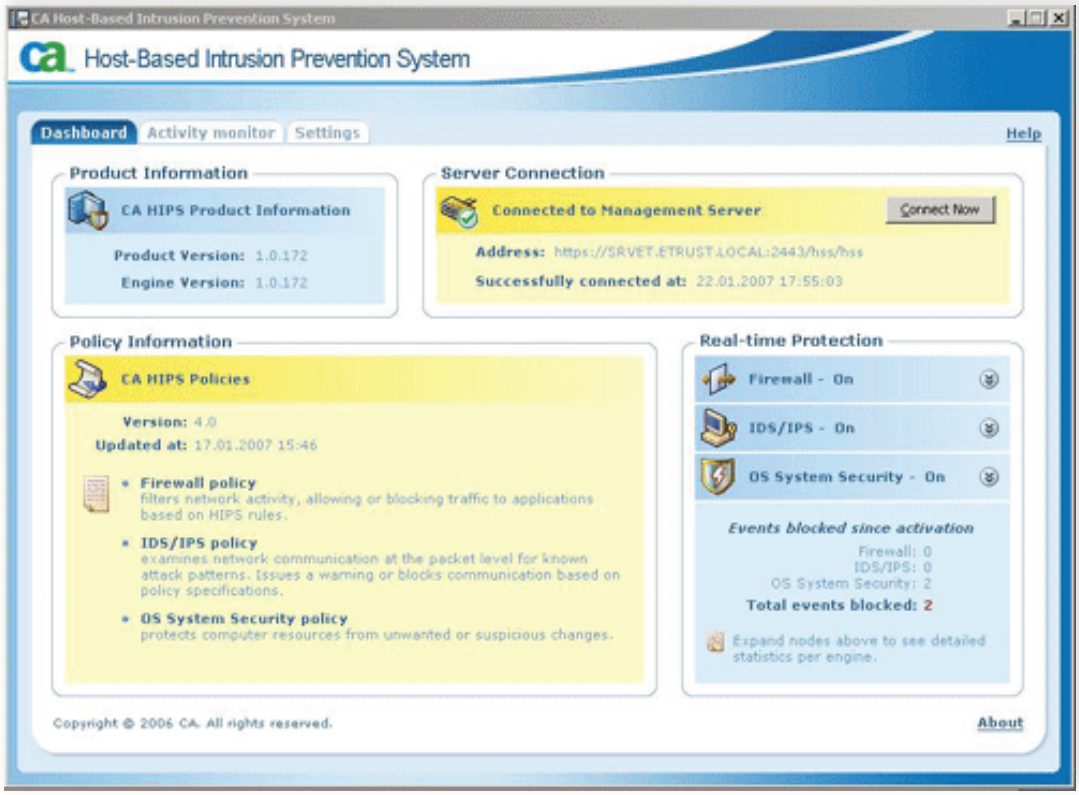


МОСКВА, 119334, УЛ. БАРДИНА, Д. 4, КОРП. 1
ТЕЛ./ФАКС: +7 (495) 925-0049, (499) 135-2519
САНКТ-ПЕТЕРБУРГ, 192007, НАБ. ОБВОДНОГО КАНАЛА, Д. 64, СТР. 2
ТЕЛ./ФАКС: +7 (812) 337-1911, 337-1912

РИСУНОК Б

Клиентский пользовательский интерфейс CA HIPS облегчает конечным пользователям блокирование новых атак на своем рабочем месте.
CA HIPS защищает ресурсы, сокращает простои и повышает эффективность работы

КЛИЕНТСКИЙ ИНТЕРФЕЙС ПОЛЬЗОВАТЕЛЯ



CA HIPS защищает ресурсы, сокращает простои и повышает эффективность работы

Используя проактивную защиту в режиме реального времени - централизованное управление доступом и принудительное применение политик безопасности в CA HIPS - вы повышаете защищенность конечной точки от известных и вновь появляющихся угроз. Программное обеспечение CA HIPS снижает риск простоев, не допуская использование конечной точки для получения доступа к сети вредоносным, шпионским и мошенническим программным обеспечением. А меньший уровень зараженности означает снижение расходов на устранение вреда и техническую поддержку в режиме "горячей линии" и более высокую эффективность работы.

Благодаря проактивному выявлению отклонений в CA HIPS, вы сможете обеспечить непрерывность обслуживания, столкнувшись с новейшими угрозами, для которых еще не был разработан механизм защиты. Воспользовавшись ключевой информацией в CA HIPS, системные администраторы смогут изучить нормальное поведение системы и создать политики для обнаружения отклонений. В результате вы сможете защитить свои ИТ-ресурсы и процессы и обеспечить их безопасную работу на время, пока будут разработаны обновленные сигнатуры. Ту же информацию можно использовать для адаптации защиты от угроз в вашей организации вместо других обходных путей.

МОСКВА, 119334, УЛ. БАРДИНА, Д. 4, КОРП. 1
ТЕЛ./ФАКС: +7 (495) 925-0049, (499) 135-2519
САНКТ-ПЕТЕРБУРГ, 192007, НАБ. ОБВОДНОГО КАНАЛА, Д. 64, СТР. 2
ТЕЛ./ФАКС: +7 (812) 337-1911, 337-1912

Адекватное обеспечение безопасности и защита от угроз является превосходной бизнес-практикой и, в зависимости от характера защищаемой информации и ИТ-ресурсов, часто обязательна по законодательным нормам отдельных штатов или федерации. Чтобы облегчить бремя обеспечения соответствия законодательным нормам, можно использовать полнофункциональные средства ведения журналов и генерации отчетов. Кроме того, CA HIPS использует уже сделанные инвестиции в традиционные защиты конечных точек системы, объединяясь с этими средствами для создания многоуровневой системы защиты от угроз, которая способна выявить и устранить угрозы, просочившиеся через один из уровней, на другом уровне.

Системные требования и поддерживаемые платформы

- Intel Xeon 3 GHz processor(s) or higher (x86/x64)
- 2 GB RAM
- 80 GB or larger hard disk
- 100/1000mbps network interface card

Поддерживаемые серверные платформы

- Windows 2000 Professional with SP4 Rollup 1
- Windows 2000 Server with SP4 Rollup 1
- Windows 2000 Advanced Server with SP4 Rollup 1
- Windows XP Professional with SP2 (32/64 bit)
- Windows 2003 Server with SP2 (32/64 bit)
- Windows 2008 Server (32/64 bit)

Минимальные системные требования

- 1.6 GHz processor
- 512MB of RAM
- 20 GB or larger hard disk

Поддерживаемые клиентские платформы

- **Windows 2000 Professional with SP4 Rollup 1**
- Windows 2000 Server with SP4 Rollup 1
- Windows 2000 Advanced Server with SP4 Rollup 1
- Windows XP Professional with SP2 and SP3 (32/64 bit)
- Windows Vista with and without SP1 (32/64 bit)
- Windows 2003 Server with SP2 (32/64 bit)
- Windows 2008 Server (32/64 bit)

Чтобы получить дополнительную информацию и увидеть, как программные решения компании CA позволяют организациям унифицировать и упростить управление ИТ-ресурсами в целях достижения более высоких результатов в бизнесе, посетите Web-страницу ca.com/products.

МОСКВА, 119334, УЛ. БАРДИНА, Д. 4, КОРП. 1
ТЕЛ./ФАКС: +7 (495) 925-0049, (499) 135-2519
САНКТ-ПЕТЕРБУРГ, 192007, НАБ. ОБВОДНОГО КАНАЛА, Д. 64, СТР. 2
ТЕЛ./ФАКС: +7 (812) 337-1911, 337-1912

Transforming IT Management