

CA Threat Manager r8.1

ПРОГРАММНЫЙ ПАКЕТ CA THREAT MANAGER ПРЕДОСТАВЛЯЕТ КОМПЛЕКСНУЮ ЗАЩИТУ ОТ УГРОЗ ДЛЯ КОНЕЧНЫХ ТОЧЕК ИТ-СИСТЕМЫ ОРГАНИЗАЦИИ С УНИКАЛЬНЫМ СОЧЕТАНИЕМ ЛУЧШИХ В СВОЕМ КЛАССЕ ПРОГРАММНЫХ ПРОДУКТОВ CA ANTI-VIRUS И CA ANTI-SPYWARE. ОПИСАННЫЕ ПРОДУКТЫ ПОЛНОСТЬЮ ИНТЕГРИРОВАНЫ В ЕДИНУЮ КОНСОЛЬ С WEB-ИНТЕРФЕЙСОМ И ИСПОЛЬЗУЮТ ОБЩИЙ КЛИЕНТСКИЙ АГЕНТ, ЧТО ОБЛЕГЧАЕТ РЕАЛИЗАЦИЮ, УПРАВЛЕНИЕ, ГЕНЕРАЦИЮ ОТЧЕТОВ И ОБНОВЛЕНИЯ.

Обзор продукта

Вредоносный код сегодня становится все более распространенным и все более сложным, а некоторые образцы даже превратились в криминальное программное обеспечение. Вы можете защитить настольные и портативные компьютеры в своей организации от этой опасности при помощи CA Threat Manager, высокоинтегрированного пакета, объединяющего в себе программные продукты CA Anti-Virus и CA Anti-Spyware. Управление этими лучшими в своем классе продуктами осуществляется через общую консоль с Web-интерфейсом, при этом используется общий клиентский агент, благодаря чему решение становится более эффективным и рентабельным.

Достоинства

Используя CA Threat Manager, вы получаете обзор любой активности вирусов или шпионских программ во всей организации как бы с высоты птичьего полета. При помощи единого графического интерфейса пользователя вы можете удаленно управлять всеми конечными точками ИТ-системы, генерировать стандартные и пользовательские отчеты и получать показатели в режиме реального времени. Развертывание не вызывает проблем, обновления эффективно используют пропускную способность сети, а администрирование не мешает конечным пользователям в выполнении их задач.

Преимущества решений CA

Решение CA Threat Manager разрабатывалось как дополнение к другим продуктам CA с целью создания многоуровневой системы защиты от различных видов угроз с централизованным управлением. Решения для обеспечения безопасности CA являются основными составляющими более общей концепции компании CA Enterprise IT Management (EITM), смысл которой заключается в упрощении и унификации развертывания, использования и интеграции всех решений и задач по управлению в контексте конкретного бизнес-направления.

CA Threat Manager защищает конечные точки ИТ-системы организации при помощи взаимоусиливающего сочетания антивирусного и антишпионского программного обеспечения

Вирусные атаки до сих пор возглавляют список наиболее дорого обошедшихся угроз в 2006 году, но шпионские программы – гораздо более зловещий и направленный вид вредоносного программного обеспечения – быстро набирают очки. Вирусописатели ищут славы и известности, тогда как многие авторы шпионских программ создают криминальное программное обеспечение для кражи информации, идентифицирующих данных и денег. Недавно проведенное анкетирование среди руководителей ведущих корпораций показало, что злонамеренные атаки всех видов составили в 2006 году до 48% всех угроз, при этом с каждым разом они становятся все более сложными и многообразными.

Традиционный «разрозненный» подход к защите от различных типов угроз при помощи решений для отдельных точек становится все менее эффективным вследствие увеличения масштаба проблемы и все более частого применения комбинированных атак, сочетающих в себе более одного вида угроз. Перед лицом непрерывно эволюционирующих методов угроз, создаваемых хорошо финансируемыми и заинтересованными в результате преступниками, вам нужны эффективные, гибкие и проактивные инструменты защиты от угроз, которые могут быстро адаптироваться к меняющемуся окружению.

Программный пакет CA Threat Manager объединяет два лучших в своем классе продукта – CA Anti-Virus и CA Anti-Spyware – в централизованно управляемое решение, предоставляющее комплексную и рентабельную защиту конечной точки ИТ-системы в сетях любого масштаба. Эта взаимоусиливающая комбинация управляется через единую консоль с Web-интерфейсом и использует общий клиентский агентский компонент, что делает реализацию, администрирование и обновления весьма эффективными. Вы получаете эффективные средства обнаружения и защиты, а также надежные средства ведения журналов и генерации отчетов и беспрецедентную поддержку языков и платформ.

РИСУНОК А

Администрирование CA Threat Manager осуществляется через консоль управления с Web-интерфейсом, которая предоставляет инструментальную панель, информацию для управления политиками и генерации отчетов для антивирусного и антишпионского модулей.

КОНСОЛЬ УПРАВЛЕНИЯ CA THREAT MANAGER

The screenshot displays the CA Threat Management Console interface. At the top, it shows the user is logged in as SILVER-2724 as administrator. The main navigation tabs include Dashboard, Discovery, Policy Management, Organization, Client, User Management, Report, and Licensing. The interface is divided into several sections:

- Virus Detections:** Shows a table of the top 10 viruses detected between Monday, October 23, 2006, and Monday, October 23, 2006. The table lists virus names and their detection counts.
- Pest Detections:** Shows a table of the top 10 pests detected in the same period, listing pest names and the number of machines affected.
- License Information:** A table showing license status, expiration dates, and node counts for eTrust Antivirus and eTrust PestPatrol.
- Product Information:** Details about the operating system (Windows XP), product version (8.1.583), service up since date, and last discover time.
- Administrator Information:** Fields for Name, Phone Number, E-mail Address, Office, Position, and Comment.

Основные средства

МНОГОУРОВНЕВАЯ СИСТЕМА ЗАЩИТЫ. CA Threat Manager объединяет в себе средства защиты от широкого диапазона угроз, включая вирусы, шпионские, рекламные и хакерские инструменты, и может интегрироваться с другими решениями CA Threat Management, такими как межсетевой экран для защиты конечных точек, серверная система защиты от вторжений, система обеспечения общей безопасности и безопасности контента.

УПРОЩЕННОЕ УПРАВЛЕНИЕ. Единая консоль управления с интуитивно понятным интерфейсом, общий клиентский агентский компонент, средства ведения журналов и сервисы обновления облегчают реализацию и администрирование и сокращают расходы на техническую поддержку.

АВТОМАТИЧЕСКОЕ И ЭФФЕКТИВНОЕ В ОТНОШЕНИИ ИСПОЛЬЗОВАНИЯ ПРОПУСКНОЙ СПОСОБНОСТИ СЕТИ ОБНОВЛЕНИЕ. CA Threat Manager обеспечивает для ваших конечных точек самую актуальную защиту при помощи автоматических обновлений сигнатур вирусов, шпионских модулей и другого вредоносного кода. Процесс обновления потребляет минимум пропускной способности системы и сети, передавая только инкрементальные обновления файла MicroDAT.

МАСШТАБИРУЕМАЯ АРХИТЕКТУРА. Решение CA Threat Manager строится на многоуровневой архитектуре с резервированием, которая не создает проблем при масштабировании, позволяя управлять крупным парком конечных точек и пользователей с единой консоли управления.

УСОВЕРШЕНСТВОВАННОЕ РАЗВЕРТЫВАНИЕ ДЛЯ МАСШТАБНЫХ СРЕД. Развертывание CA Anti-Spyware можно выполнить при помощи любой сторонней программы поставки программного обеспечения, в том числе, CA Unicenter® Software Delivery и Microsoft Systems Management Server. Вы можете обеспечить эффективное и безопасное развертывание системы во всей организации, используя уже сделанные инвестиции в средства поставки программного обеспечения.

ПОДДЕРЖКА MICROSOFT VISTA. CA Threat Manager предоставляет сертифицированную поддержку ОС Microsoft Vista для настольных компьютеров.

РАСШИРЕННАЯ ПОДДЕРЖКА ПЛАТФОРМ. CA Anti-Virus обеспечивает самую широкую поддержку имеющихся операционных систем для конечных точек. Поддерживаются многие версии Windows, а также Macintosh, UNIX, Linux и NetWare.

ШИРОКАЯ ПОДДЕРЖКА РЕГИОНАЛЬНЫХ ЯЗЫКОВ. Используя CA Threat Manager, вы получаете самую широкую поддержку региональных языков, включая английский, французский, итальянский, немецкий, испанский, японский, бразильский вариант португальского языка и традиционный и упрощенный варианты китайского языка.

УСОВЕРШЕНСТВОВАННАЯ ЭВРИСТИКА. Используя технологию эвристического сканирования с расширенными возможностями, приложения могут просматривать загрузочные сектора и файлы, удаляя вредоносное содержимое из данных в процессе обработки и восстанавливая инфицированные системы до защищенного и безопасного состояния.

ГИБКИЕ ПАРАМЕТРЫ ОСМОТРОВ. Управление осмотрами осуществляется с центральной консоли управления и может выполняться автоматически в запланированное время или при подключении пользователя к сети. Дополнительный агентский интерфейс пользователя позволяет запускать осмотры и просматривать их журналы в соответствии с политикой компании.

ВЗАИМОДЕЙСТВИЕ ПО ИНИЦИАТИВЕ АГЕНТСКОГО КОМПОНЕНТА. Взаимодействие между агентом и консолью происходит по инициативе агента, то есть он может заранее связаться с консолью, сообщить о своем состоянии и получить новые политики и конфигурационные изменения.

УВЕДОМЛЕНИЯ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ. Вы получаете автоматические уведомления при обнаружении в среде события, имеющего отношение к новой угрозе, это событие заносится в журнал, и вы можете удалить вредоносную программу в режиме реального времени. «Белый список», или файлы исключений, для санкционированных приложений можно тонко настроить для отдельных пользователей или подразделений компании, чтобы предотвратить ложные срабатывания.

НАДЕЖНЫЕ СРЕДСТВА ГЕНЕРАЦИИ ОТЧЕТОВ. Разнообразные отчеты, которые можно использовать без какой-либо предварительной настройки, позволяют отобразить информацию в удобном для чтения графическом формате, что облегчает задачи администрирования, а также выявления и решения проблем. Вы можете генерировать ежечасные, ежедневные, еженедельные, ежемесячные и ежеквартальные отчеты, а также отчеты для отдельных машин или пользователей.

ПОДДЕРЖКА ПРОГРАММНЫХ ПРОДУКТОВ CISCO NAC И MICROSOFT NAP Подключаемый модуль CA Posture Plug-in для Cisco NAC и CA System Health Agent для Microsoft NAP собирают важную информацию о текущем состоянии безопасности для продуктов CA, установленных в сетях, защищаемых системами Cisco NAC и Microsoft NAP.

РАСШИРЕННОЕ ИССЛЕДОВАНИЕ УГРОЗ. CA Threat Manager поддерживается подразделением CA Security Advisor, надежным источником информации по безопасности с 1987 года. Группа CA Security Advisor укомплектована исследователями мирового класса, которые ведут непрерывающийся круглосуточный мониторинг на предмет возникновения новых угроз, а также разрабатывают новые процедуры для их ослабления и устранения.

НЕЗАВИСИМАЯ СЕРТИФИКАЦИЯ. CA Threat Manager имеет сертификаты ICSA LABs и West Coast Labs и постоянно завоевывает награды "VB 100%" от журнала Virus Bulletin за 100-процентное выявление существующих в реальной среде вирусов. Программный продукт CA Anti-Spyware, помимо этого, прошел сертификацию West Coast Labs.

РИСУНОК В

Агент CA Threat предоставляет сводную, статистическую информацию и информацию по типу журналов для антивирусного и антишпионского модулей.

АГЕНТ CA THREAT MANAGER

Component	Install Status	Realtime Status	Release
Antivirus Agent	Installed	On	8.1.583.0
PestPatrol Agent	Installed	On	8.1.583.0

Antivirus Information

- License: Valid Subscription.
- Time Remaining: 15 day(s) until next license check.
- Update your License Information here.
- Antivirus Engine Version: 30.3.0.0
- Signature Version: 30.3.3152.0
- Last Signature Update: 10/23/2006
- Change your Update Settings here.
- Realtime Protection: On
- Change your Realtime Settings here.

PestPatrol Information

- License: Valid Subscription.
- Time Remaining: 15 day(s) until next license check.
- Update your License Information here.
- PestPatrol Engine Version: 5.6.8.13
- Signature Version: 2006.10.20.16
- Last Signature Update: 10/23/2006
- Change your Update Settings here.
- Realtime Protection: On
- Change your Realtime Settings here.

Copyright © 2006 CA. All rights reserved.

CA Threat Manager обеспечивает защиту в режиме реального времени и одновременно облегчает администрирование и управление расходами

Используя CA Threat Manager, ваши администраторы получают инструменты, необходимые для повседневного и эффективного управления широким диапазоном угроз. Единая консоль с Web-интерфейсом предоставляет интегрированный обзор "с высоты птичьего полета", способствуя повышению эффективности работы и сокращению или даже устранению расходов на исправление вреда и содержание службы поддержки в форме "горячей линии".

Автоматически выявляя и удаляя вирусы, шпионские, рекламные и другие вредоносные программы, которые могут инфицировать вашу сеть, решение CA Threat manager сокращает риск простоев, позволяет вашим сотрудникам спокойно продолжать работу, что способствует обеспечению бесперебойного обслуживания. Уведомления в режиме реального времени и проактивные обновления добавляют еще один уровень защиты ИТ-ресурсов от атак с использованием вновь обнаруженных уязвимостей, для которых еще не разработаны механизмы защиты.

Расширенные средства генерации отчетов и ведения журналов помогают быстро выявить и нейтрализовать угрозу, кроме того, их можно использовать для того, чтобы содействовать исследованиям и соблюдению требований законодательства.

В целях расширения диапазона механизмов защиты от угроз, все программные продукты компании CA для обеспечения безопасности являются взаимодополняющими, поэтому CA Threat Manager можно использовать в сочетании с другими продуктами CA, в том числе, с решением CA Host-Based Intrusion Prevention System, которое объединяет в себе автономный межсетевой экран и средства обнаружения и предотвращения вторжений, и CA Secure Content Manager, решением для управления безопасностью контента, построенном на использовании правил и защищающем организацию от передачи во внешние сети частной информации. Эти компоновочные блоки защиты от угроз можно реализовать постепенно, создавая многоуровневую систему защиты, которая будет обладать беспрецедентными возможностями в защите вашего сетевого окружения от существующих и вновь появляющихся угроз.

РИСУНОК С

Подразделение CA Security Advisor обеспечивает круглосуточный глобальный мониторинг и быстрое реагирование на нарушения системы безопасности.

CA SECURITY ADVISOR

The screenshot shows the CA Security Advisor website. At the top, there is a navigation bar with links for SOLUTIONS, SUPPORT, NEWS, EVENTS, ABOUT CA, INVESTORS, WORLDWIDE, and BUY. The main header features the CA logo and the text "CA Security Advisor" with a search box. Below the header, a "Welcome to the CA Security Advisor site" message is displayed, followed by a brief description of the service. A "SECCON" warning box indicates a "Warning" level for the real-time global security condition. To the right, there are promotional banners for "Buy eTrust® PestPatrol® Anti-Spyware" and "Large Enterprise" solutions. The main content area is divided into two columns: "Spyware Information Center" and "Virus Information Center". Each column has a "Latest Alerts" section and a "Free Scan" button. The "Virus Information Center" also includes an "RSS" link and a "View all" button. On the right side, there is a "Search" section with a search box and a "GO" button, and an "Online Tools" section with a "Free Spyware Scan" button.

ПРОДУКТ	ФУНКЦИЯ	ОСОБЕННОСТИ	ПРЕИМУЩЕСТВА
CA Threat Manager	Защищает организации от вирусов, шпионских и других вредоносных программ; использует общую консоль управления с Web-интерфейсом и клиентский агентский компонент	<ul style="list-style-type: none"> • Препращает путь вредоносному программному обеспечению • Централизованное управление • Высокая степень масштабируемости • Средства ведения журналов и генерации отчетов • Поддержка различных платформ 	<ul style="list-style-type: none"> • Сокращает простои • Повышает производительность • Возможность глобального развертывания • Способствует соблюдению законодательных требований • Помогает в управлении расходами

Системные требования и поддерживаемые платформы

Клиентский компьютер

- Процессор Pentium 150 или выше, 64 Мбайт свободного дискового пространства и 512 Мбайт оперативной памяти
- Windows NT 4.0, SP6A или более поздние версии
- Windows 2000
- Windows Server 2003
- Windows XP Professional
- Windows Vista Desktop

Управляющий сервер

- Процессор Pentium 4 2.6 Мгц или выше, 10 Гбайт свободного дискового пространства и 1 Гбайт RAM
- Windows NT 4.0, SP6A или более поздние версии
- Windows 2000 Server
- Windows 2003 Server
- Windows XP Professional
- Windows 2000 Workstation
- Windows Vista OS

Примечание: ОС Windows XP Professional и Windows 2000 Workstation не рекомендуется использовать вследствие их ограничения на десять одновременных соединений.

Дополнительная поддержка платформ для решения CA Anti-Virus

- Linux (32-разрядные версии): Red Hat Enterprise Linux 3 и выше, SuSE Linux Enterprise Server 8 и выше, SuSE 9.0 и выше
- UNIX: Sun Solaris 8 и выше; HP-UX 11.0 и 11.11
- Novell: NetWare 5.1 и выше

- Citrix Presentation Server 4 for Windows
- Lotus: Notes/Domino 4.6.2 и выше
- Использование в сети устройств NAS: Использование навигатора по файловой системе
- Cisco NAC и Microsoft NAP Support for Windows
- Apple: Macintosh OS X 10.3 и выше для Power PC; Macintosh OS X 10.4 и выше для Intel
- Шлюз: Microsoft Windows NT 4.0, 2000, XP, 2003 и Red Hat Linux
- Подключаемый модуль шлюза: Microsoft ISA Server; Apache; CVP
- Микрокомпьютеры (КПК): Palm, Microsoft Windows Mobile 2002/2003/2005, Microsoft Smartphone 2005 и Pocket PC 2003

Преимущества решений CA

Как и остальные решения от компании CA, CA Threat Manager можно интегрировать с другими продуктами CA и решениями сторонних компаний для обеспечения комплексного и всестороннего управления разнообразными ИТ-средами. Все продукты построены на платформе интеграции CA, которая представляет собой набор совместно используемых сервисов, в том числе, рабочих потоков, правил, политик, пользовательского интерфейса и информации для управления. Общая база данных представляет собой коллективные знания, которые могут использоваться для информации и операций в различных предметных областях управления. CA Threat Manager и другие решения для обеспечения безопасности от компании CA являются ключевыми составляющими инициативы CA под названием EITM, смысл которой заключается в унификации и упрощении всей среды управления информационными технологиями в организации. Используя сервис-ориентированную архитектуру, EITM предоставляет комплексные интегрированные средства управления всеми аспектами информационных технологий в контексте конкретного направления бизнеса. Эта инициатива переводит управление ИТ-системами на новый, беспрецедентный уровень, объединяя компоненты управления угрозами в единое целое, в результате чего мы получаем интегрированное решение, предоставляющее гораздо больше возможностей, чем простая сумма всех компонентов. Мы можем сократить риски, управлять расходами, совершенствовать сервис и увязывать инвестиции в ИТ-системы с приоритетами бизнеса.

Дальнейшие шаги

CA Threat Manager представляет собой взаимоусиливающую комбинацию программ CA Anti-Virus и CA Anti-Spyware, тесно связывающее эти два лучших в своем классе программных продукта под управлением общей консоли и клиентского агентского компонента, что способствует рационализации управления и расходов.

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.

